Internet Safety Technical Task Force
Technology Submission Template

Gemalto, Inc./ Neville Pattinson CISSP CIPP
http://www.gemalto.com

Abstract
Putting Parents in control at the point of access is the key to protecting minors on the Internet. Smart Cards are a proven technology for ensuring authenticated access control to on-line services. Preserving the identity of minors and ensuring a safe internet experience is achievable in a cost effective manner. By ensuring an age verification policy is presented by the accessing party to remote services, a simple mechanism can be deployed between the server and the accessing client to ensure internet content access is adjusted to the accessing party's requirements. By creating a workable scheme which puts the accessing party (e.g. parent) in control ensures the protection of minors on-line.

Keywords
Smart Cards, Authentication, Privacy, Security, Age Verification Service.

Functional Goals
Please indicate the functional goals of the submitted technology by checking the relevant box(es):
☑ Limit harmful contact between adults and minors
☑ Limit harmful contact between minors
☑ Limit/prevent minors from accessing inappropriate content on the Internet
☑ Limit/prevent minors from creating inappropriate content on the Internet
☑ Limit the availability of illegal content on the Internet
☑ Prevent minors from accessing particular sites without parental consent
☑ Prevent harassment, unwanted solicitation, and bullying of minors on the Internet
☐ Other – please specify

PROBLEM INTRODUCTION
Online Internet safety for minors is achievable with existing technologies today along with an access control policy. The combination of both can provide a safe internet experience at a cost effective price. Missing today in our society is a mechanism to determine a person's identity and their age on access or application to internet content. Simple attempts are made today but are easily worked around by the increasing sophistication and knowledge of minors as they grow up in our Information and connected age. Considering internet content servers can be located anywhere in the world, a local or national law will likely be ineffective at controlling or policing the access rights of individuals. One fundamental question that needs to be answered is how to determine who is trying to access a service online and are they who they say they are. On top of this determination a scheme in needed to present authenticable age related information in order to control access/content. Without a strong ubiquitous identity management system on the internet we must consider a different mechanism to protect minors from obtaining access to inappropriate content or being exposed to other vulnerabilities. In addition, the inability to provide age verification attributes with any trusted identity verification information cannot allow remote services to adjust served content according to age limitations. Smart Cards can be used to authenticate identity and present age policy information. Age policy information becomes a key aspect of achieving the goal of controlled access to content. Importantly minor's identities also need to be protected online. By providing a mechanism to protect their identity and also provide age verification policy to the site being accessed, the online services can ensure they uphold and enforce the age appropriate content policy. The accessing client and smart card devices will ensure the remote site is configured with the age verification scheme and will block all content if the site does not authenticate it's participation in the scheme. By involving the parents first and equipping them with low cost hardware identity security technology they can put protective measures in place for their children. These efforts must go hand in hand with the cooperation of internet content providers. Providers that do not participate will have all content blocked by the client. Implementing a hardware based solution at the client makes any attempts to overcome the security and access policy enforcement significantly stronger than a software only approach.

PROPOSED SOLUTION
Smart cards, either in card form or USB token form factor, are highly established in the field of presenting identity securely and are highly effective at preserving and enhancing privacy. Smart Cards are proven devices which are a convenient mechanism to authenticate the user and their identity when interacting with web sites.

By first creating an effective Identity and Access control Policy for internet service access, identity management and access policy can then be utilized to control access and content to minors. Access control to websites can be maintained by the presentation of electronic credentials maintained in secure smart cards based hardware devices.

The first step is to equip parents with the right tools. This would require creating and activating an Age Verification Service on their internet access points. With the use of

smart cards or USB variants they would then configure identity and access policies into the device(s). The devices would be required to be present (e.g. a dongle) when accessing remote services. The remote servers would then be equipped simply with suitable functionality that would detect the incoming access request and be able to detect that Age Verification Service (AVS) was required by the incoming party. The user then authenticates their presence to their smart card by PIN or biometric authentication which in turn transmits account identity and AVS policy information to the remote server. The server must then accommodate and enforce the AVS policy according to their content for this specific user. The site will be required to authenticate back to the user's smart card device to indicate participation in the AVS scheme. Any clients equipped with AVS will not allow access to any site that does not support AVS once it is enabled at the access point.

Parents, application providers and Internet content providers must all cooperate together to create a safe and appropriate internet experience for minors. Sites that don't cooperate will be blocked by the accessing client by default. By equipping both applications and internet content servers with the ability to determine if the accessing party has Age Verification Service enabled (i.e. the accessing party is enforcing protective measures from their access point). The servers can then interact with the accessing party and establish account identity (or persona) authentication resulting in the delivery of age restriction policy from the access party to the online service. The online service can then determine access policy according to the presented request from the secure hardware based smart card devices controlling the user's access.

EXPERTISE

Gemalto is a world wide leader in Digital Security. Our mission is to provide cost effective smart card based solutions to our customers that can provide secure access to physical and logical facilities and services. We participate in international standards and national standards bodies to promote open standards in all areas of our business, such as identity authentication, travel documents, financial transactions, transportation systems, and mobile telecommunications.

COMPANY OVERVIEW

Gemalto is a $2.2 billion leader in digital security, providing secure and easily deployable strong authentication personal devices, platforms and solutions in the private and public sectors. Gemalto is the result of a recent merger of Axalto & Gemplus.

With operations in 100 countries and 10,000 employees, including 1,500 R&D engineers, Gemalto's solutions are designed to make personal digital interactions more convenient, secure and enjoyable. More than a billion people worldwide use the company's products and services for telecommunications, financial services, e-government, identity management, multimedia content, digital rights management, IT security, mass transit and many other applications.

BUSINESS MODEL OVERVIEW

Opportunities exist for several entities in this proposal. There are several models that can be used for deployment of smart identity card credentials to minors; one being a commercial organization such as an internet content provider or identity broker promoting and enforcing the Age Verification Service. It is possible this could be a not-for-profit organization providing a manageable scheme for parents and minors. In any model the parent would need to obtain a commercially available AVS kit which would enforce parental access policy for internet access with hardware devices (smart cards). These devices would act as the local security agent in their minor's hands enforcing their parent's access policies for internet content. Purchase of the devices could be provided through retail outlets or by subscription to a service provider. Internet content providers would be equipped with simple readily available access control functionality on their servers which would work in conjunction with the user's access requests and their AVS security devices.

MORE INFORMATION

www.gemalto.com
www.secureidcoalition.org
www.smartcardalliance.org

CONTACT INFORMATION

Neville Pattinson CISSP CIPP
VP Government Affairs & Business Development
Gemalto, Inc,
Austin, TX, USA
Email: Neville.Pattinson@gemalto.com

CERTIFICATION

I certify that I have read and agree to the terms of the Internet Safety Technical Task Force Intellectual Property Policy.

REFERENCES

None