WebFort Advisory – Update on the latest Web Browser and Adobe Flash Releases

v0.2_July28_2011

This document outlines the new privacy enhancing features that were introduced in recent releases of web browsers and Adobe Flash and how they can affect CA Advanced Authentication technologies. It lists the possible impact on end-user experience and suggests alternate strategies that can be adopted to adjust.

Background

CA Technologies offers strong authentication solutions that include the use of multi-factor credentials. One of the multi-factor user credentials is the CA ArcotID. The CA ArcotID includes a PKI private key that is protected using a patented technology and a PIN known only to the real user that can unlock this protected private key. Users authenticate to the portal with a combination of the ArcotID (something they have) and the PIN (something they know).

CA WebFort is the versatile authentication server that supports a variety of credentials – CA ArcotID being one of them. Other credentials include ArcotOTP, Password, Questions and Answers (QnA), hardware tokens, and virtual OTP (one time passwords) that are delivered via SMS, voice or emails.

The CA ArcotID is a preferred credential, because it provides the most natural interface and experience for the user (username/password prompts), while providing superior security. The CA ArcotID can be delivered and stored on the user's desktop using a variety of client software – Adobe Flash, JavaScript, Java Applet and an installed Native Client. The Adobe Flash client is popular because it is transparently downloaded without user interaction.

Recent Software Releases

Older versions of the web browsers allowed the user to easily remove the browser cookies, but not the Flash objects. Users who wanted to remove Flash objects had to explicitly use a Flash tool and remove them. Newer versions of browsers have enhanced the users' ability to control privacy settings and allows them to more easily block browser cookies and Flash objects) and remove them once they are set.   The affected versions are listed in the table below -

Software	Version(s)
Adobe Flash	10.3
Internet Explorer	8 and 9
Firefox	4 and 5
Chrome	12

With the recent software releases, Flash objects are treated the same as cookies – using the browser option to remove cookies also removes Flash objects. Previous software releases of the browser and Flash had allowed users to opt for an "in-private" mode in which the browser blocked the setting of persistent cookies and Flash objects.

Cookies and Flash objects

Websites have generally used browser cookies and Flash objects to "remember the user" on a device and provide an enhanced consumer experience. Websites use this to automatically log users in, provide a personalized experience based on what the user had done in previous visits, allows users to continue from where they left off, etc. The security model of cookies and Flash objects allows sites to restrict access to these markers so other sites cannot see or use these markers.

Users have always had the choice of using the browser option and deleting cookies. Between a quarter and one third of the users periodically delete cookies. Others prefer the convenience of letting the cookies be – and benefit from the enhanced experience when they visit their favorite sites. Very few users (less than 10%) regularly delete their Flash object store – many did not even know how to use the Flash tool and delete the objects.

The CA WebFort authentication server stores the CA ArcotID on the user's device in a number of formats. The client type and the corresponding storage approach are shown in the table below.

Client Type	CA ArcotID Storage Format	Client Installed
Adobe Flash	Flash Secure Object - FSO	No
JavaScript	Browser Cookie	No
Unsigned Java Applet	Browser Cookie	No
Signed Java Applet	File on filesystem	Yes
Native Client	File on filesystem	Yes
Adobe Reader/Acrobat	File of filesystem	Yes

The Flash client provides a seamless user interface by storing the ArcotID as a Flash secure object that persists in the user's device.

Impact of the new software releases

The recent web browser and Flash releases do not impact the working of the Arcot technology. However, the user's choice of system settings could have an impact on the user experience. For instance, browsers can be configured to delete cookies and Flash objects when the browser is closed. When this happens, the CA WebFort authentication server will not recognize the user or his device and will use the roaming flow to validate the user through QnA , a voice or SMS-based OTP, or other secondary authentication method.

Some other situations that may cause this experience include:

- Strengthen privacy settings – Users may strengthen privacy settings in the browser or in other 3rd party software like Anti-virus software (which also include anti-malware, anti-adware and other capabilities). These settings may block the creation of browser cookies or Flash objects. The settings override the "remember me" option that the user may click in the website – so users will be confused by why the system does not "remember" them.
- Clearing cookies – Users may manually clear cookies or opt for a setting in the 3rd party Endpoint protection suites (anti-virus) that periodically clears cookies. With the new browser and Flash versions, the Flash objects holding the CA ArcotID will be deleted too. Users who previously experienced continuity through Flash objects will suddenly see that they are being put in "roaming" flow more frequently.

Roaming, per se, is not an issue. Most sites have support for roaming and allow the user to either download the ArcotID on the fly or use a backup credential. However, users who find themselves in roaming flow when they don't expect it may panic and call the help desk or simply abandon the transaction. Depending on the roaming method (e.g. OTP via SMS, OTP via voice, QnA), backup credential and the frequency, users may get very frustrated.

Options for customers

CA Technologies customers have a couple of options to address the situation.

1. Communicate – Customers can communicate information about the new software to their users. Most users may not realize that a cookie or Flash object is being placed on their device. By design most websites use non-technical terms like "remember me" to get the user's consent to place the cookie or Flash object. Users may not correlate the "privacy settings" in their browser or Anti-virus software to the "remember me" option at their bank site. By informing users about the interplay of these software components and the potential impact on their experience, banks and other enterprises will help users avoid the panic and resultant calls to help desk or abandonment.
2. Add Java signed applet to their website – The Java signed applet stores the ArcotID as a file which is not impacted by the privacy settings on browsers or endpoint protection (anti-virus) products. Also, the ArcotID file is not deleted when cookies or Flash objects are deleted explicitly or implicitly by the clean-up operations of other 3rd party software. Comparison of the Flash and other ArcotID clients is provided below.

Client	Benefits	Considerations
Flash	No software install. Transparently downloaded when user visits website	Flash not available in a very small number of devices. So plan a backup approach – JavaScript, for example. Flash objects deleted easily with new versions of browser or Flash. So users will be routed to roaming flow
Java Signed Applet	ArcotID stored as file – not susceptible to easy deletions ArcotID can be "locked" to device – so works only on that device and cannot be coped over No admin privileges required to install the software. Downloaded easily from web site.	Signed applet will prompt for user's permission – once – to install itself. Very, very small number of devices may not have Java installed. So plan a backup approach, JavaScript, for example.
Native Client	ArcotID stored as file – not susceptible to easy deletions ArcotID can be "locked" to device – so works only on that device and cannot be coped over Download once. Optionally add CSP and other interfaces to support digital signing and encryption	Installable software will prompt for user's permission – once – to install itself Optional CSP interfaces may require admin privileges

Summary

Software – browsers, Flash, etc. – are all being modified to provide better privacy control to users. The side effect of these enhancements is the ability for users to block the setting of cookies and Flash objects on their devices, and the ability for users to easily remove the cookies and Flash objects. Users may explicitly remove cookies or Flash objects or create settings in browsers and 3rd party software (e.g. anti-virus software) that allows them to be blocked or deleted. Users may in many cases, be unaware of what they have done.

The CA ArcotID Flash client deploys the CA ArcotID user credential as a Flash object. Recent changes to browsers and Adobe Flash may result in users unknowingly blocking or deleting the CA ArcotID credential causing them to have a different user experience than they expect. Users who face this may become frustrated or concerned, which increases helpdesk call volumes or even abandonment of the strong authentication technology.

CA Technologies customers must educate their users about the possible impact of their actions. Customers must also consider the option of adding other clients (Signed Java or Native) to deploy the CA ArcotID as a file and avoid the unplanned roaming situation.