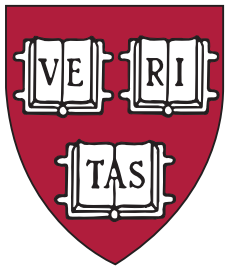
HARVARD
UNIVERSITY



Information Technology

Integer Alternate Secure Login

Thursday, March 20, 2014

The Harvard Integrated Management System - Project Integer[1]
Alternate Secure Login

Version	Date	Description	Contributors
1.0	March 14, 2014	Initial version.	Jon Saperia
1.1	March 17, 2014	Revisions based on review by Scott Bradner	Jon Saperia
1.2	March 20, 2014	Revisions based on input from Dave Taylor	Jon Saperia
1.3	March 20, 2014	Additional edits to terms based on input from Scott Bradner	Jon Saperia

Introduction

Integer is designed to support a number of standard authentication approaches and systems such as CAS, the focus of our first release. At the same time, Integer must function in the event of a failure of this or other similar systems. To address this requirement, Integer supports a method of direct support to our front end servers that will bypass the standard Web page sequence that touches the authentication server before the browser contacts Integer.

For most users, this facility will be unavailable and/or unknown. This document describes how this facility will work.

Normal Operation

In normal operation the user enters a URL in their browser that will take them to the specified resource in Integer. If the 'application cookie'[2] is current and valid, they will be granted access. In the case of a user that has invalid or absent, the steps are as follows:

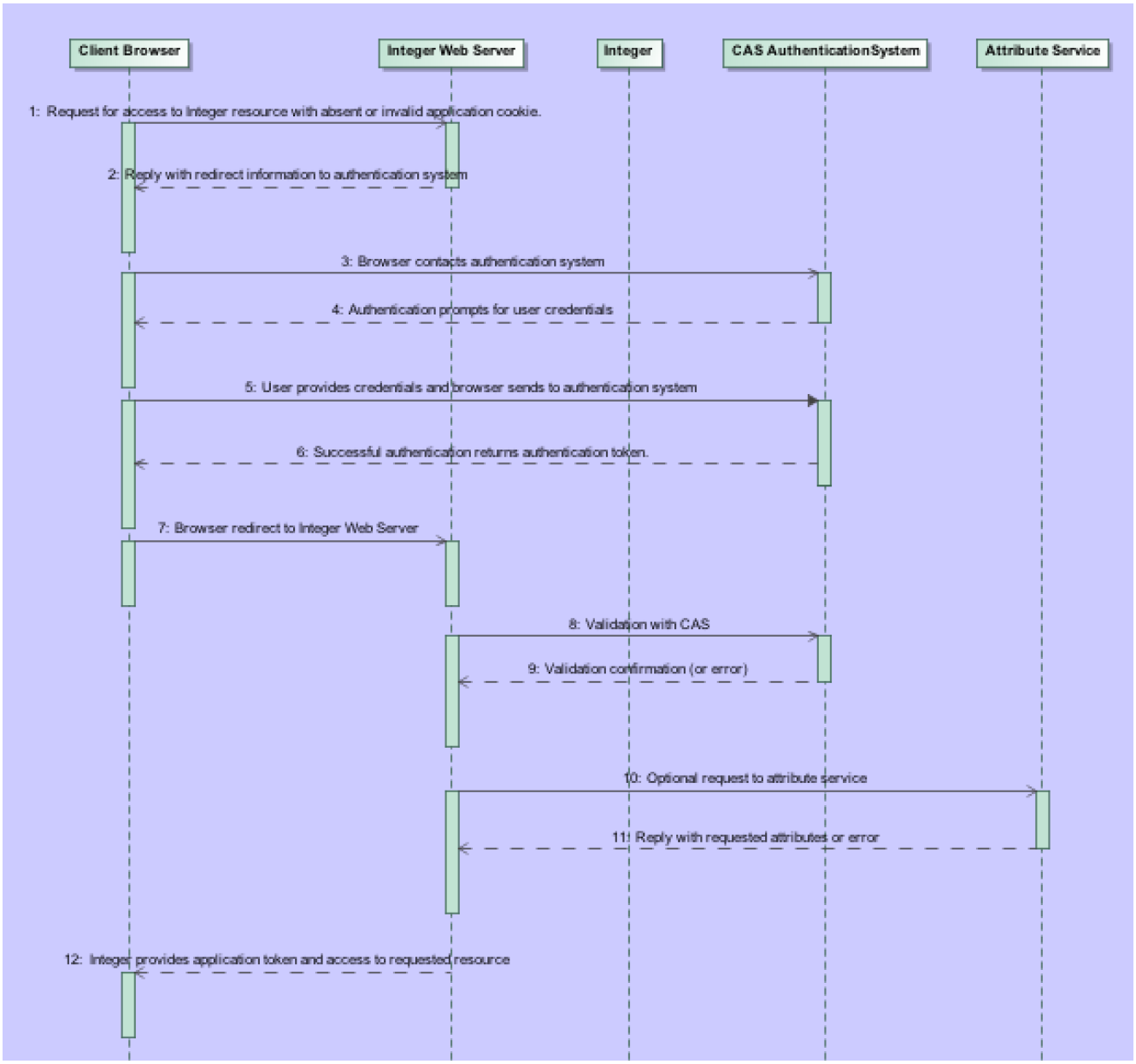
1. User makes access request to a resource in Integer.
2. The Integer Web server provides a reply to the browser with redirect information to the authentication system.
3. Browser contacts authentication system
4. The authentication system prompts the user to enter their credentials.
5. User enters credentials and browser sends them to the authentication system.

---

[1] The project, Integer, is an attempt to create a unified whole from the separate protocols, data elements and software systems we use to operate our increasingly complex computing environments. See: http://www.thefreedictionary.com/integer. Also see: http://en.wiktionary.org/wiki/integer#Latin

[2] In this case, an application cookie is used to mean the cookie that Integer creates after the user has been successfully been authenticated by the authentication system.

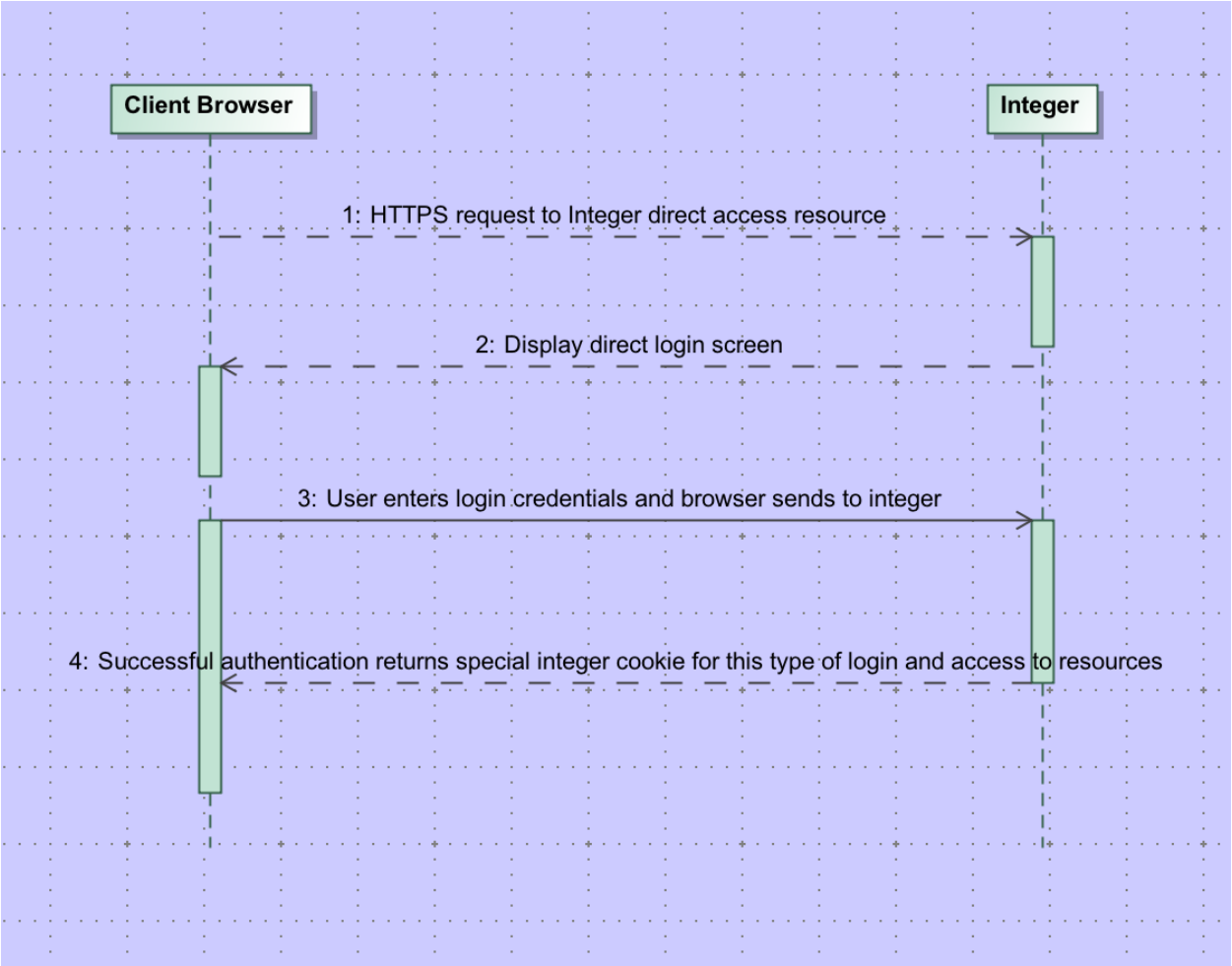
6. Authentication system replies with valid authentication token (or an error).
7. Successful authentication causes the user to be redirected to the Integer Web server.
8. The Integer Web server validates with CAS.
9. CAS returns with validation (or error).
10. If configured to use an attribute service, Integer may optionally make a request to an attribute service (e.g., for information about employment status).
11. Attribute service returns to Integer and Integer makes final determination about granting access to requested resource.
12. Integer Web server will put the Integer application token in the browser, the user will



granted access to the resource.

Alternate Login

Integer is intended to manage the entire infrastructure including authentication systems and attribute services. For this reason, Integer provides an alternate login facility for a few highly trusted users so that in the event of the failure of an attribute or authentication system, access to Integer is maintained.



Note that in the sequence diagram above, user credentials (a user ID and password) are exchanged between the browser and Integer in contrast to the ‘normal’ approach.