Brief Version - Authentication Focus Group (AFG) Report Regarding Ex Libris' Plan to Terminate Support for Alma Internal Password Authentication

---

Background

At the September 2016 IGelU meeting, Ex Libris announced its plans to move toward the use of external-only password management in Alma. This shift would affect customers' ability to create patron and staff accounts where the password is stored within Alma. A joint ELUNA/IGeLU External Authentication Focus Group (AFG) was formed to work with Ex Libris to determine the best course forward.

In subsequent meetings between the AFG and Ex Libris it was confirmed that Alma external-only authentication was not a requirement of the ISO/IEC 27018 (Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.) This was cited by Ex Libris as the reason users needed to move away from using internal passwords. Rather, the need for Alma external-only authentication is a suggested best practice that Ex Libris would like to strictly adhere to the practice.

The AFG developed the *"Alma Password Authentication Survey: Assessment"* tool to assess how each Alma institution is using password control within Alma. Additionally, the AFG wanted to determine the degree of impact a move to external-only authentication would have on institutions.

This report presents findings from the survey and offers recommendations to Ex Libris, the IGeLU and ELUNA Steering Committees, and the Alma community as potential next steps.

Summary

Nearly a quarter of Alma institutions contracted for, in implementation, or in production (193 of ~700) responded to the Authentication Focus Group's (AFG) survey. This is a statistically significant survey result that the AFG feels is an adequate reflection of the overall Alma community.

Over 75% of survey respondents indicated that they use internal authentication exclusively or a mix of internal and external authentication. It is likely that every institution has at least one internal account to allow an institutional "backdoor" should there be problems with external authentication. Every institution has at least one internal account for Ex Libris staff. Ex Libris indicated that they would create an external authentication system for Ex Libris accounts, so these will no longer be a concern. Over 50% of the respondents use shared/generic accounts and 72% have community users authenticated internally, because their institution's external authentication can't handle these types of users or their institution doesn't have external authentication at all. The most critical use cases for internal authentication in Alma are those institutions that do not have the capacity or are bound by policy or regulations to authenticate users internally.

The second part of the survey was to gauge interest in possible solutions. While almost 31% of respondents indicated that the use of social media authentication might be a possible alternative to internal authentication, nearly 70% responded negatively to this solution. Very few institutions indicated passwordless authentication as a viable option, but given the questions received about this option, it is possible that the concept is not well known among respondents. The majority of respondents indicated they could not move their internally authenticated users to their central authentication service because the users were not affiliated with their institution.

The answers to the survey preparedness questions indicated that more than a third of the respondents would likely not be able to move entirely to external authentication before the end of 2018, largely because of scheduling, costs, capacity, and maybe even desire. To be fair, institutions couldn't provide more exact time estimates for a migration without knowing what the solutions would be or what help would be provided.

The survey was designed to gauge impact and readiness regarding an anticipated move away from internal authentication. The numeric results tell only a partial story. Many, but not all, institutions should be able to handle a move to external authentication depending on the potential solutions, although not likely as quickly as Ex Libris would like the move to happen. However, textual responses, answers to in-depth interview questions, and unsolicited calls and email correspondence via ALMA-L indicate to the AFG that there is widespread unhappiness, frustration, and sometimes anger regarding this issue. The AFG strongly encourages Ex Libris staff to take the time to read all comments.

Ex Libris staff acknowledge that the announcement of the move could have been handled better. Institutions were unaware that the release of a new social media authentication integration was not just an option, but was intended as a likely means for institutions to move away from internal authentication. Apparently, support staff mentioned the move in an answer to a customer, forcing Ex Libris to announce this "required" move at IGeLU. As is often the case, communication did not move swiftly through the company and sales and support reportedly were still telling customers they could use internal support even after the IGeLU conference.

Some institutions commented that internal authentication was one of the reasons they bought Alma. They do not have capacity nor do they want to move away from internal authentication (e.g. *We do not have the infrastructure or resources to employ an alternate authentication system.*) Many others cannot engage their own IT staff or central IT in setting up a new authentication system (e.g. *Ex Libris has always stated that Alma would mean less local ICT support will be required -- this new direction in password control means that ICT support is now needed again*.) The AFG heard a small number of comments from institutions who thought this might be a breach of contract (e.g. *We only use internal accounts. According to our procurement we asked for a system with the possibility to create accounts for our users with username and password.*) and more who considered the removal of internal authentication as a loss of functionality. Finally, there were comments directed at Ex Libris including the following from a member of a consortia *"I have lost faith in Ex Libris."*

The AFG acknowledges that some institutions, such as the State Library of Queensland, already have on their forward IT plan the migration of all Alma accounts to external only. The shift in password management by Ex Libris means that this may occur sooner than later.

While the AFG fully understands the security benefits to an all-external authentication system, we also understand that the work involved in such a move would be extensive, and in some cases not possible, for institutions. The AFG feels it is important that Ex Libris read all comments and take them to heart when considering the path forward.

Recommendations

Given that the move to external-only authentication is an industry best practice and not a certification requirement for Ex Libris, we do not feel a move to external authentication should be made mandatory for institutions already contracted for, in implementation, or live on Alma, especially if there are circumstances that make the move challenging. Based on the survey results, interviews, and discussions with Ex Libris, the AFG recommends the following:

1. The AFG or other standing committee should continue to work with Ex Libris to develop a list of viable potential solutions and migration paths for institutions that desire to move to external-only authentication. A suggested list of solutions, including potential issues and specifications should be available to institutions no later than the end of Q1 2017. Ex Libris might also consider partnering with customers as part of a pilot to establish a migration and maintenance process. These early adopters could act as champions for such a move..
2. Ex Libris should consider hosting an external authentication system in order to make the transition from internal authentication seamless to the user community. This would obviate concerns institutions have about contracting with a third party. The benefit is clear: ownership and management of authentication work would be supported by Ex Libris, while user and password management would still be under the control of institutions.
3. Ex Libris should continue to pursue alternative access via external authentication to allow local institutional administrators as well as Ex Libris staff to access Alma without relying on the institutional central authentication system.
4. The move to external authentication should not be mandatory for those institutions contracted for, in implementation, or production for Alma.