

Re: customer authentication center

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-02/msg00702

- *From:* DaveMo <david.mowers@xxxxxxxxxx>
 - *Date:* Fri, 15 Feb 2008 07:42:16 -0800 (PST)
-

On Feb 13, 2:05 am, "Sergei Karimov" <OverDrone_Tr...@xxxxxxxx> wrote:

Hi, Guru!

There are several company web sites (ASP.NET) that use forms authentication. For now each web site has it's own customer (web site end user) login/password database.

The idea is to merge all login info into one secure repository. There are several benefits: customers will be able to use single login for all web sites, simplified administration and others...

In future some web sites and customers will use certificates to login and/or perform critical operations, so this center must support PKI.

I googled and found MS Product – ADAM (Active Directory Application Mode), standalone LDAP repository. And there are several questions that I couldn't find info in documentation:

1. Is MS ADAM appropriate for this task?
2. Is it possible to set up several instances of ADAM that share same repository using synchronization (similar to AD)?
3. How password in LDAP repository stored – in clear text or encrypted (let's say by some one way hash)? If it's encrypted, what algorithm is used and is it possible to change it?
4. Has certificate based authentication (in PKI) anything to do with LDAP and ADAM? If there is no any integration then some additional module/delegate must be implemented to route authorization request based on type (certificate based authorization is routed to PKI CA and login/password based authorization is routed to ADAM via LDAP)...
5. Is it possible to store in ADAM repository such information as (per application or web site): user roles, grants? What are the common practices to store and manage this kind of data in LDAP repository such as ADAM?
6. Are there any problems setting up LDAP over SSL?

I would appreciate to receive an answer to any question...

I agree with all of the answers above, except that if you are seriously going down the path of a certificate-based authentication system you may want to consider setting up regular AD instead of ADAM. AD provides deep integration with server-side Schannel (the SSL

Re: customer authentication center

authentication package) to properly validate a client certificate and map it to a user account. The mechanism is very flexible, but well tested and secure. If you went the ADAM route, you'd have to write (or have someone write) the mapping function for you. There seems little good reason to do this since it is built in to AD/Windows/IIS.

Maybe someone has a good reason not to use a separate AD for customers, but I'm not aware of any real blocking issues.

HTH,
Dave

.