Microsoft®
Desktop Optimization Pack
for Software Assurance

MBAM Self-Help Portals

Authoring a self-help portal workflow for BitLocker Recovery Using Microsoft BitLocker Administration and Monitoring (MBAM)

Technical White Paper

Published: September 2011

Priyaa Nachimuthu and Nathan Barnett

Microsoft®

CONTENTS

Situation

Microsoft BitLocker Administration and Monitoring (MBAM) customers might want to author key recovery portal which is customized for their enterprise with MBAM

Solution

Understand the APIs and type of data available in MBAM to design and develop custom key recovery portal with a case study

Benefits

- Leverage the base foundation provided by MBAM to encrypt computers and store recovery key information
- Custom key recovery portal to suit the needs of your enterprise

Products & Technologies

- Microsoft Windows Server 2008
- BitLocker Drive Encryption in Windows 7
- Microsoft BitLocker Administration and Monitoring
- Windows Communication Foundation
- SQL Server 2008

EXECUTIVE SUMMARY

The purpose of this whitepaper is to help customers who want to design their custom key recovery portal for their enterprise. It outlines how to use Microsoft BitLocker Administration and Monitoring (MBAM) APIs to recover keys stored by MBAM with the help of a case study.

This paper assumes that readers are familiar with BitLocker Drive Encryption and Windows Communication Foundation technologies.

INTRODUCTION

Bit Locker Drive Encryption (BDE) is a Windows security feature that is used by enterprise customers to secure their data on corporate assets - portable devices in particular. BitLocker Drive Encryption allows you to encrypt all the data stored on the Windows operating system volume and configured data volumes. It also ensures the integrity of early boot components by using Trusted Platform Module (TPM).

Microsoft Bit Locker Administration and Monitoring (MBAM) provide features to manage BitLocker encryption of computers in an enterprise. BitLocker creates recovery information at the time of encryption and MBAM stores the same in the recovery data store. This recovery information is required when BitLocker-protected drives need to be recovered in the event that the specified unlock method cannot be used (such as if the TPM cannot validate the boot components, the personal identification number (PIN) is forgotten, or the password is forgotten). In these instances, the user must be able to provide the recovery password to unlock the encrypted data on the drive. Similarly prior to enabling BitLocker on a computer with a TPM version 1.2, TPM must be initialized. The initialization process generates a TPM owner password, which is a password set on the TPM. The user must be able to supply the TPM owner password to change the state of the TPM, such as when enabling or disabling the TPM or resetting the TPM lockout. For more information about Microsoft BitLocker Administration and Monitoring (MBAM), see the MBAM product documentation (http://go.microsoft.com/fwlink/?LinkId=218349).

MBAM provides means to retrieve recovery information or TPM information for a computer on behalf of a user from the data store via MBAM administration portal. However, you might want a custom portal to enable self-help scenarios or to have a user interface to audit and report statistics at regular intervals. This whitepaper will provide guidelines to design a custom portal for recovery and TPM retrieval using MBAM including understanding of the helpdesk feature and the helpdesk WCF web service interfaces provided by MBAM. It also includes an example that outlines the design of a custom recovery portal using MBAM web service interfaces.

UNDERSTANDING THE MBAM HELPDESK FEATURE

MBAM provides an administration web interface to enable helpdesk users to recover key or TPM information on behalf of users. The primary component of the Helpdesk feature includes MBAM Administration web service that enables the communication between the administration web interface and MBAM data store.

MBAM Helpdesk Components

The MBAM Administration web service enables the MBAM administration portal or a third-party tool to query recovery and TPM information from the data store. The MBAM administration portal will provide the user interface and controls to enable the helpdesk-user to retrieve key or TPM information for a computer on behalf of the user.

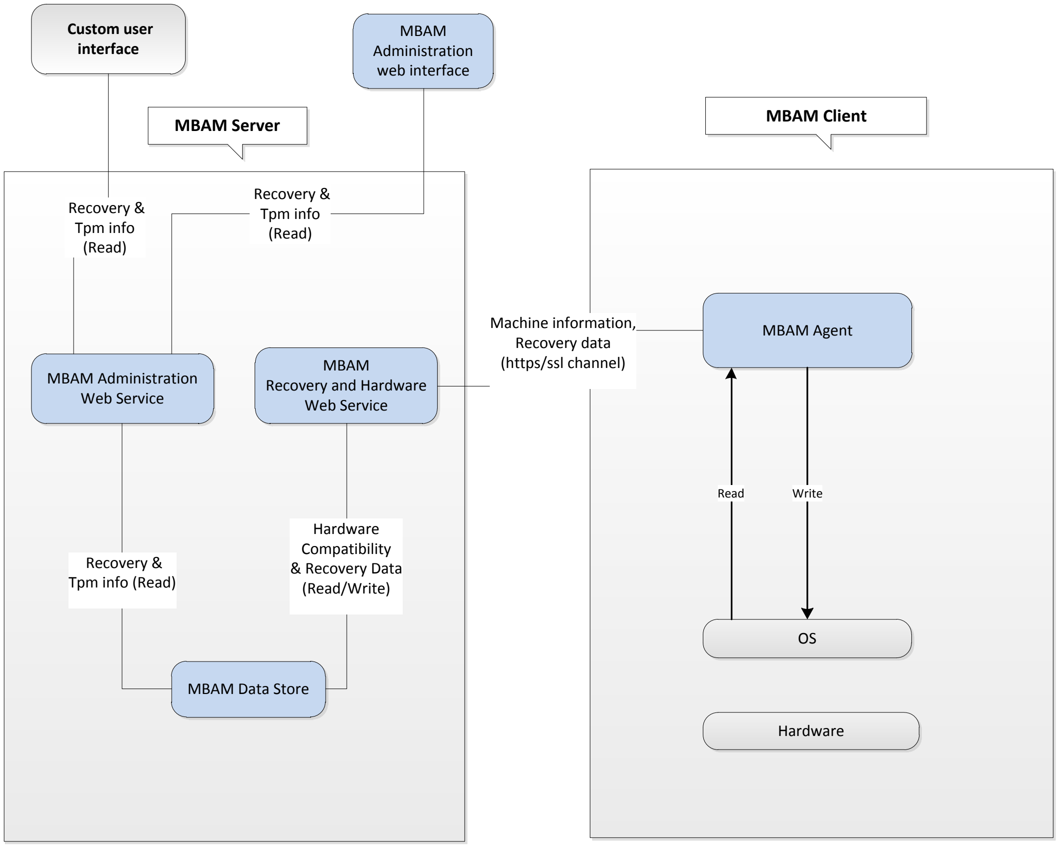
Custom user interface
MBAM Administration web interface
MBAM Server
MBAM Client
Recovery & Tpm info (Read)
Recovery & Tpm info (Read)
Machine information, Recovery data (https/ssl channel)
MBAM Agent
MBAM Administration Web Service
MBAM Recovery and Hardware Web Service
Read
Write
Recovery & Tpm info (Read)
Hardware Compatibility & Recovery Data (Read/Write)
OS
MBAM Data Store
Hardware

Figure 1. MBAM Helpdesk feature design

MBAM agents installed on client computers send recovery and TPM information along with computer and user information to MBAM Recovery and Hardware web service when the encryption process starts. MBAM Recovery and Hardware web service stores this information in the MBAM Recovery data store.

The MBAM Administration web portal uses MBAM Administration web service interfaces to retrieve recovery and TPM information from the data store. The MBAM Administration web portal provides access to two types of users: helpdesk users and advanced users. Helpdesk users need to provide user information along with a recovery key ID to obtain the recovery key on behalf of the user. An advanced user must provide only the recovery key ID to obtain the recovery key. A helpdesk user must provide both the user and computer information to obtain the TPM owner password whereas an advanced user only needs to provide the computer information to obtain the TPM owner password.

UNDERSTANDING MBAM RECOVERY INTERFACES

To develop your custom web portal to recover key or TPM information you must understand MBAM web service interfaces. MBAM Administration web service is a WCF web service that provides four web service interfaces for recovery keys and two web service interfaces to recover TPM owner password. MBAM also provides auditing for key and TPM recovery with these web service interfaces. Whenever a recovery key or TPM owner password is requested via the web interfaces, the MBAM Administration web service logs the request information in the MBAM reporting data store for auditing purposes.

MBAM Key Recovery Interfaces

The MBAM Administration WCF web service provides the following four web interfaces to retrieve recovery key for a user.

RecoveryKeyData GetRecoveryKey (string recoveryKeyId, string reasonCode, string requestorUserName, string requestorDomainName);

This method is intended for an advanced user and expects the whole recovery key ID along with reason for this key request, requestor name and domain name. In the case of MBAM Administration portal, requestor is helpdesk user who is requesting a recovery key on behalf of the user. The reason could be a lost pin, a lost startup key, a BIOS change, a TPM reset, a lost passphrase, a lost smartcard, an operating system boot order change etc. This method searches the recovery data store for a recovery key matching the given recovery key ID and returns RecoveryKeyData which contains the recovery key ID, volume GUID, recovery key, recovery package if any, computer name, computer domain name, list of device users and last updated time.

RecoveryKeyData GetRecoveryKeyForUser (string recoveryKeyId, string userName, string userDomainName, string reasonCode, string requestorUserName, string requestorDomainName);

This method is intended for a helpdesk user and expects the whole recovery key ID, the computer user name and the user domain name along with reason for this key request, the requestor name, and the domain name. In the case of MBAM Administration portal, the requestor is a helpdesk user who is requesting on behalf of the user and the reason could be a lost pin, a lost startup key, a BIOS change, a TPM reset, a lost passphrase, a lost smartcard, an operating system boot order change etc. This method searches the recovery data store for a recovery key matching the given recovery key ID, and the user information and returns RecoveryKeyData which contains the recovery key ID, the volume GUID, the recovery key, the recovery package if any, the computer name, the computer domain name, a list of device users, and the last updated time.

string[] GetRecoveryKeyIds (string partialRecoveryKeyId, string reasonCode, string requestorUserName, string requestorDomainName);

This method is intended for an advanced user and expects a partial recovery key ID (first 8-36 characters) along with reason for this key request, the requestor name and the domain name. In the case of MBAM Administration portal, the requestor is a helpdesk user who is requesting on behalf of the user and the reason could be a lost pin, a lost startup key, a BIOS change, a TPM reset, a lost passphrase, a lost smartcard, an operating system boot order change etc. This method searches the recovery data store for a set of matching recovery key

IDs matching the given partial recovery key ID and returns a list of matching recovery key IDs.

string[] GetRecoveryKeyIdsForUser (string partialRecoveryKeyId, string userName, string userDomainName, string reasonCode, string requestorUserName, string requestorDomainName);

This method is intended for a helpdesk user and expects a partial recovery key ID (first 8-36 characters), the computer user name and the user domain name along with the reason for this key request, the requestor name and the domain name. In the case of MBAM Administration portal, the requestor is a helpdesk user who is requesting on behalf of the user and the reason could be a lost pin, a lost startup key, a BIOS change, a TPM reset, a lost passphrase, a lost smartcard, an operating system boot order change etc. This method searches the recovery data store for a set of matching recovery key IDs matching the given partial recovery key ID and returns a list of matching recovery key IDs.

MBAM TPM Recovery Interfaces

MBAM Administration web service provides the following two web interfaces to retrieve TPM owner password.

TpmRecoveryData GetTpmHash (string computerName, string computerDomainName, string reasonCode, string requestorUserName, string requestorDomainName);

This method is intended for an advanced user and expects the computer name and the computer domain name along with the reason for this TPM owner password request, the requestor name and the domain name. In the case of MBAM Administration portal, the requestor is a helpdesk user who is requesting on behalf of the user and the reason could be a reset pin lockout, TPM has been turned on, TPM has been turned off, a change in the TPM password, a clear TPM etc. This method searches the recovery data store for the TPM owner password matching the given computer information and returns TpmRecoveryData which contains TPM owner password, a list of device users and the last updated time.

TpmRecoveryData GetTpmHashForUser (string computerName, string computerDomainName, string userName, string userDomainName, string reasonCode, string requestorUserName, string requestorDomainName);

This method is intended for a helpdesk user and expects the computer name, the computer domain name, the computer user name and the user domain name along with the reason for this TPM owner password request, the requestor name and the domain name. In the case of MBAM Administration portal, the requestor is a helpdesk user who is requesting on behalf of the user and the reason could be a reset pin lockout, TPM has been turned on, TPM has been turned off, a change in the TPM password, a clear TPM etc. This method searches the recovery data store for the TPM owner password matching the given computer information and returns TpmRecoveryData which contains the TPM owner password, a list of device users and the last updated time.

EXAMPLE

The IT department of Tasmanian Traders wants to deploy MBAM to manage BitLocker encryption of corporate data on their enterprise computers. They also want to provide a self-help portal for a user to recover keys or TPM owner password without calling the helpdesk. They decide to design a Recovery Portal using the MBAM infrastructure.

Recovery Portal Scenarios

The following are some of the scenarios for BitLocker Key or TPM owner password recovery for the IT department of Tasmanian Traders. They need to deploy MBAM to manage BitLocker protection of corporate data. However, the IT department doesn't have many resources available for helpdesk support, so they need to support the scenario where a user who has lost his pin or password is able to recover the recovery key by himself via the portal. They also need to let the user's manager and the administrators of that particular computer know that the recovery key was requested.

- The Helpdesk user can recover the recovery key when a user calls the helpdesk when the user loses the pin or password for a computer or when the user cannot login in to the Recovery Portal
- The Helpdesk user can recover the recovery key by providing user credentials and the whole or a partial recovery key ID
- Helpdesk user can recover the TPM owner password when a user calls and requests for one
- The Helpdesk user can recover the TPM owner password by providing the computer information, and the user information
- A user can recover recovery key when he loses his pin or password and is directed to a recovery console that provides the recovery key for the computer and prompts for a recovery key
- A user requesting recovery information must be authenticated using smart card and PIN to confirm user identity.
- A user can recover recovery key by providing the whole or a partial recovery key ID
- A user can recover the TPM owner password by providing computer information
- A user can read frequently asked questions when he needs help using the portal
- The user's manager and last logged on administrator of the computer will receive notification email when a recovery request is made
- An IT administrator can view reports on usage statistics of the portal

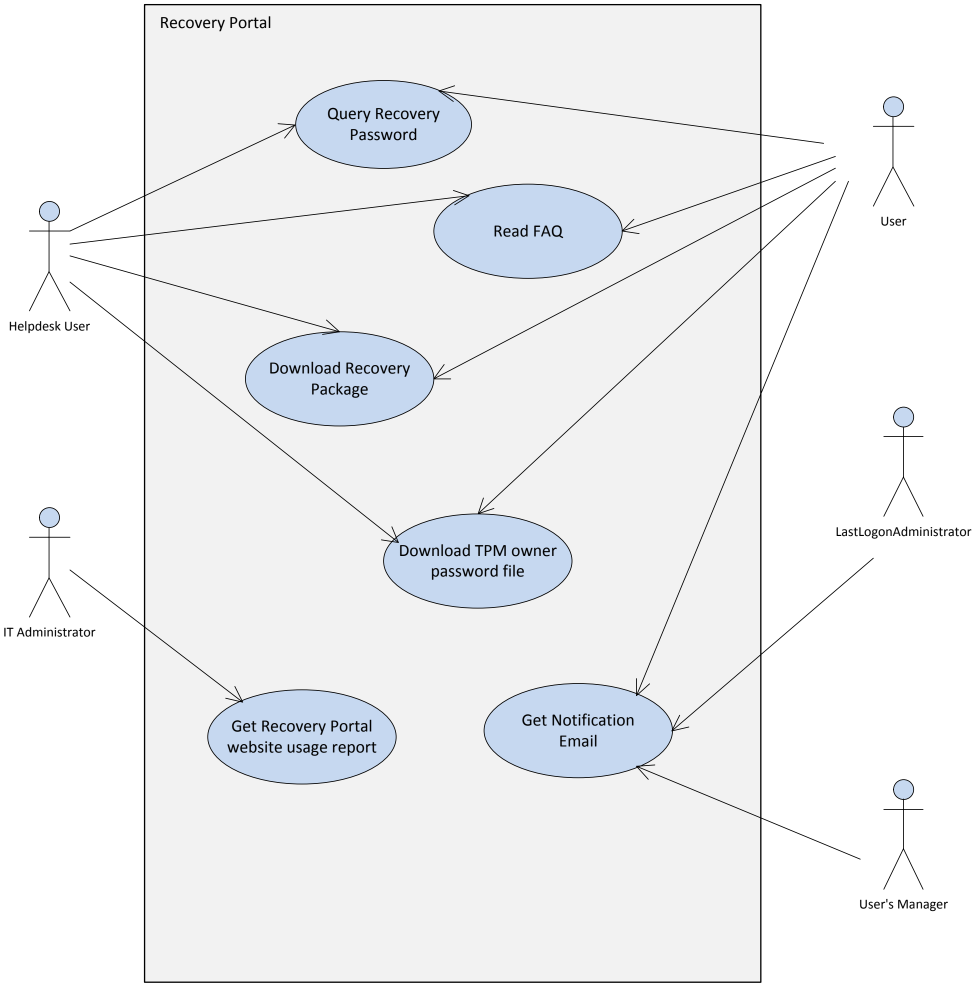

Figure 1. Recovery Portal use cases

Interaction between Helpdesk user and Recovery portal

A user does not have smart card and PIN so the user cannot use the Recovery Portal and must call the Helpdesk to get recovery information. The Helpdesk user visits the Recovery Portal when a user loses the pin or password for his computer and cannot login into the Recovery Portal. Once the Helpdesk user's credentials are validated, the recovery page is displayed to the Helpdesk user. The Helpdesk user's credentials are validated per enterprise policy standards (for instance by being part of a security group with access to Recovery Portal). A helpdesk user must validate the requesting end user's identity per standard operating procedures of Tasmanian Traders before providing the end user with the recovery password. The helpdesk user enters user information and a partial recovery key ID provided by the user and then picks a matching recovery key ID returned by the recovery page and then submits the request. The recovery page provides the recovery key and the associated recovery package that can be downloaded by Helpdesk user. The recovery password is provided to the end user per existing password delivery policy standard (Email, vmail etc.).

The helpdesk user visits the Recovery Portal when a user loses the pin or password for his computer. Once the Helpdesk user's credentials are validated, the recovery page will be displayed to the helpdesk user. The helpdesk user enters the computer and user information provided by the user and submits the request. The recovery page returns TPM owner password file associated with the information and can be downloaded by Helpdesk user.

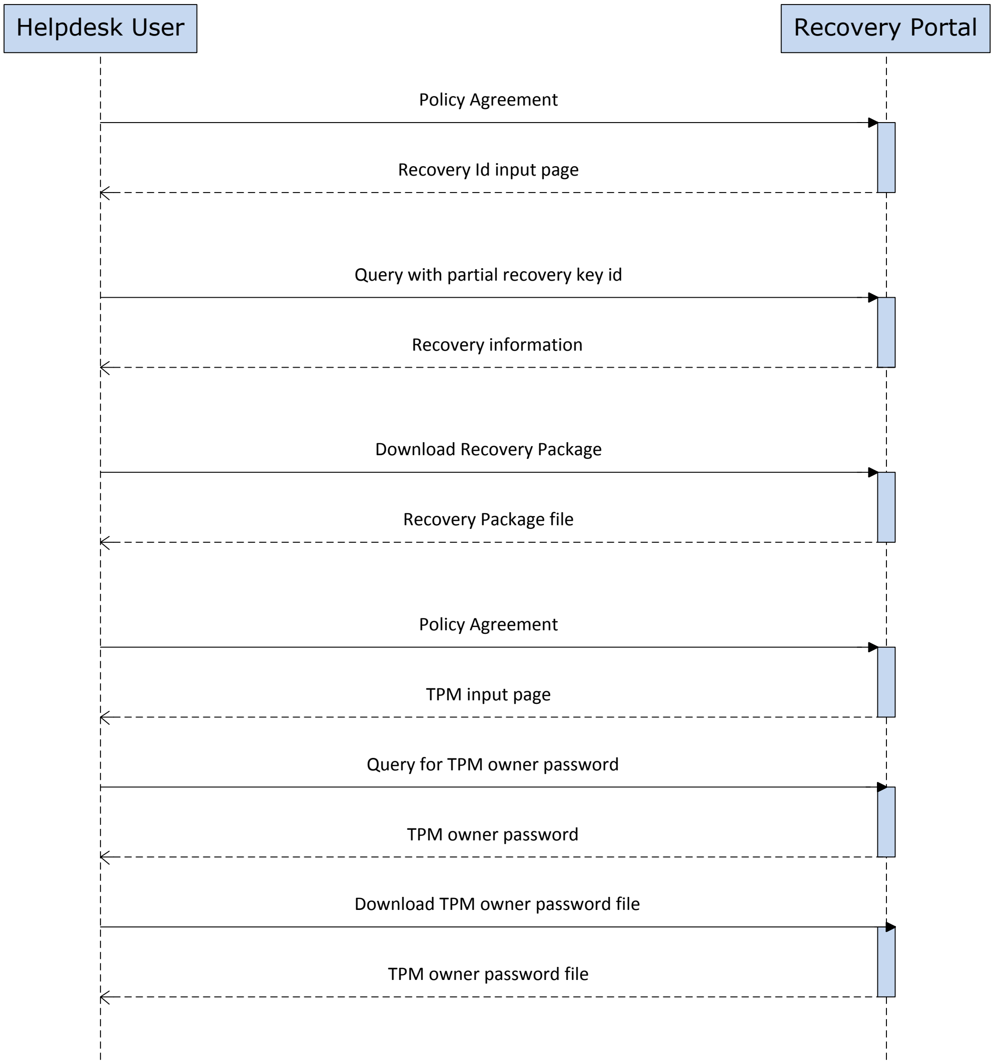

Figure 2. Work flow for interaction between the helpdesk user and the Recovery Portal

Interaction between user and Recovery portal

A user has a smart card and PIN to access the Recovery Portal and he visits the Recovery Portal when he loses his pin or password for his computer. Once the user’s credentials are validated using smart card authentication per enterprise policy standards, the recovery page is displayed. The user enters a partial recovery key ID or whole recovery key ID from the recovery console, picks a matching recovery key ID returned by the recovery page, and then submits the request. The recovery page provides the recovery key and associated recovery package that can be downloaded by the user. The user can print this data from the Recovery Portal or email it to himself. Email is automatically sent to the smart card authenticated user and user’s manager to notify them of the request.

If user does not have an alternate computer to log-on to and uses the computer of an already logged in user (i.e. colleague, manager) to access the web portal, then the application should determine the logged-in user differ from the user requesting access to the web site. The user should be prompted for smart card ID so that smart card credentials can be entered and, if possible, capture the smart card user’s identity. The logged-on user does not need to match credentials of the smart card authenticated user. Web portal authentication is limited to smart card. If the smartcard user’s identity cannot be captured, network authentication can be used. Revocation status of the smart card certificate must be checked.

Any user with access to the 8-digit partial recovery key ID and a smart card and PIN can access the associated recovery password and recovery key package. The request is logged in the data store for audit by a MBAM administrator and email notification is sent to the smart card authenticated user, last logged-on administrator and the user’s manager that a request has been made.

The user visits the Recovery Portal when he loses the pin or password for his computer. Once the user’s credentials are validated with smart card authentication, the recovery page is displayed to the user. The user enters the computer information and submits the request. The recovery page provides the TPM owner password file associated with the parameters and can be downloaded by the user.

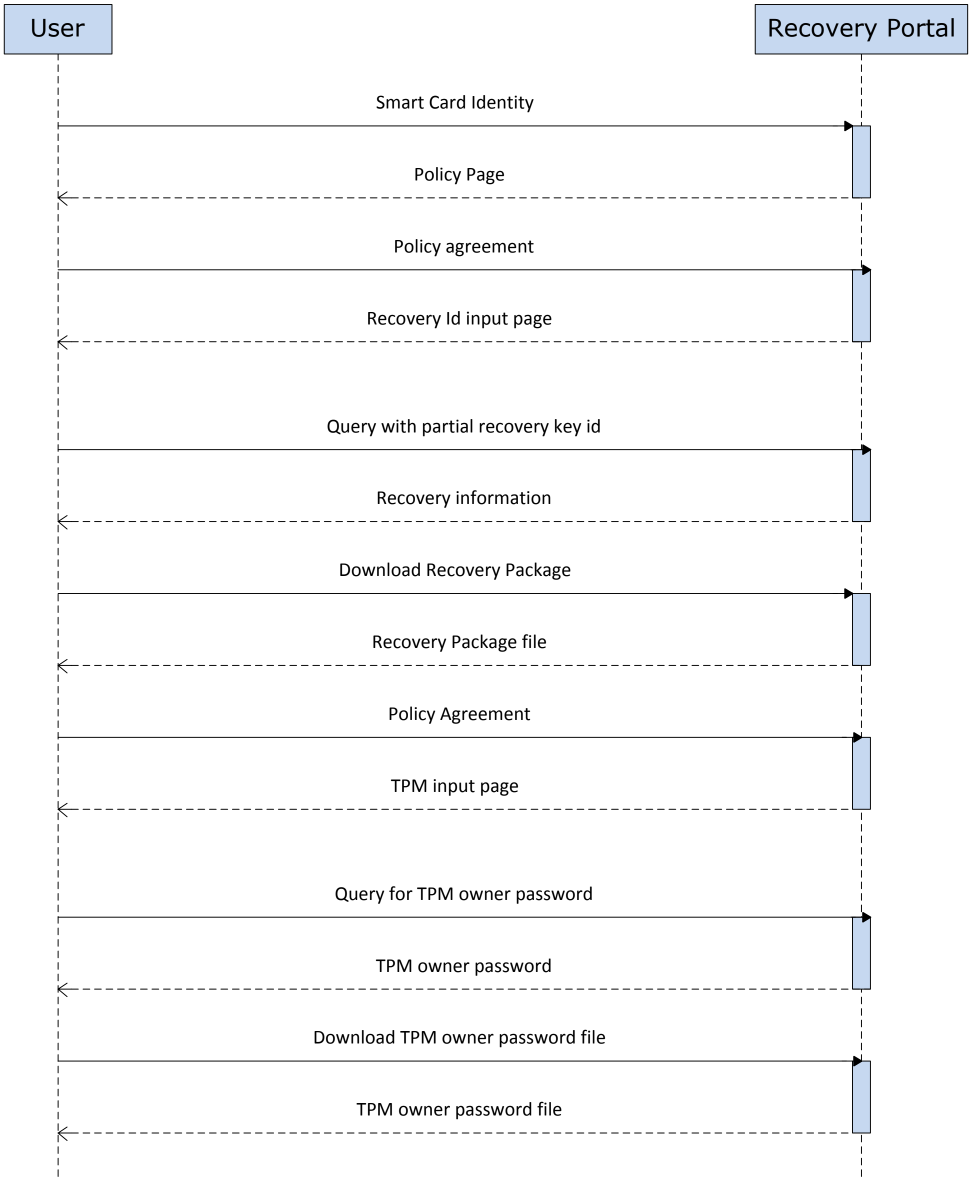

Figure 3. Work flow for interaction between user and Recovery Portal

Recovery Portal with MBAM

The following shows the interaction between Recovery Portal and MBAM via a UI controller. When a user requests a recovery password by providing a partial recovery key ID, the UI controller calls the MBAM GetRecoveryKeyIds interface which returns a set of matching recovery key IDs. When the user picks a recovery key ID, the UI controller will pass the complete key ID by calling the GetRecoveryKey interface which returns the recovery key information in RecoveryKeyData. The UI controller passes the recovery key and recovery package information to the user. The UI controller also obtains the user's manager alias and last- logon administrator information and sends an email notification that a recovery key was requested by the user for that particular computer.

When a user requests a TPM owner password by providing the computer information, the UI controller calls the MBAM GetTPMHash interface which returns the TPM owner password file in TPMRecoveryData. The UI controller passes the TPM owner password to the user. The UI controller also obtains the user's manager alias and last- logon administrator information and sends an email notification that a TPM owner password was requested by the user for that particular computer.

Every Key or TPM request is logged in the data store by MBAM for auditing. The recovery Portal will use the audit information in the data store to display reports of recovery requests on the reports page. This report provides a summary of information on system usage for a specified date range. Report from-date and to-date filters are provided to allow administrators to choose a specific date range. Report from-date and to-date filters are populated with the current date by default. The following information is included in the report, using standard SQL REPORTING SERVICES format.

- Report Data
- Total number of requests.

Total number of requests can be further categorized into total number of requests by end users, by help desk users, by IT administrators or by number of keys. Further classification will include successful retrievals, unsuccessful retrievals or list of key ID retrievals by each user group.

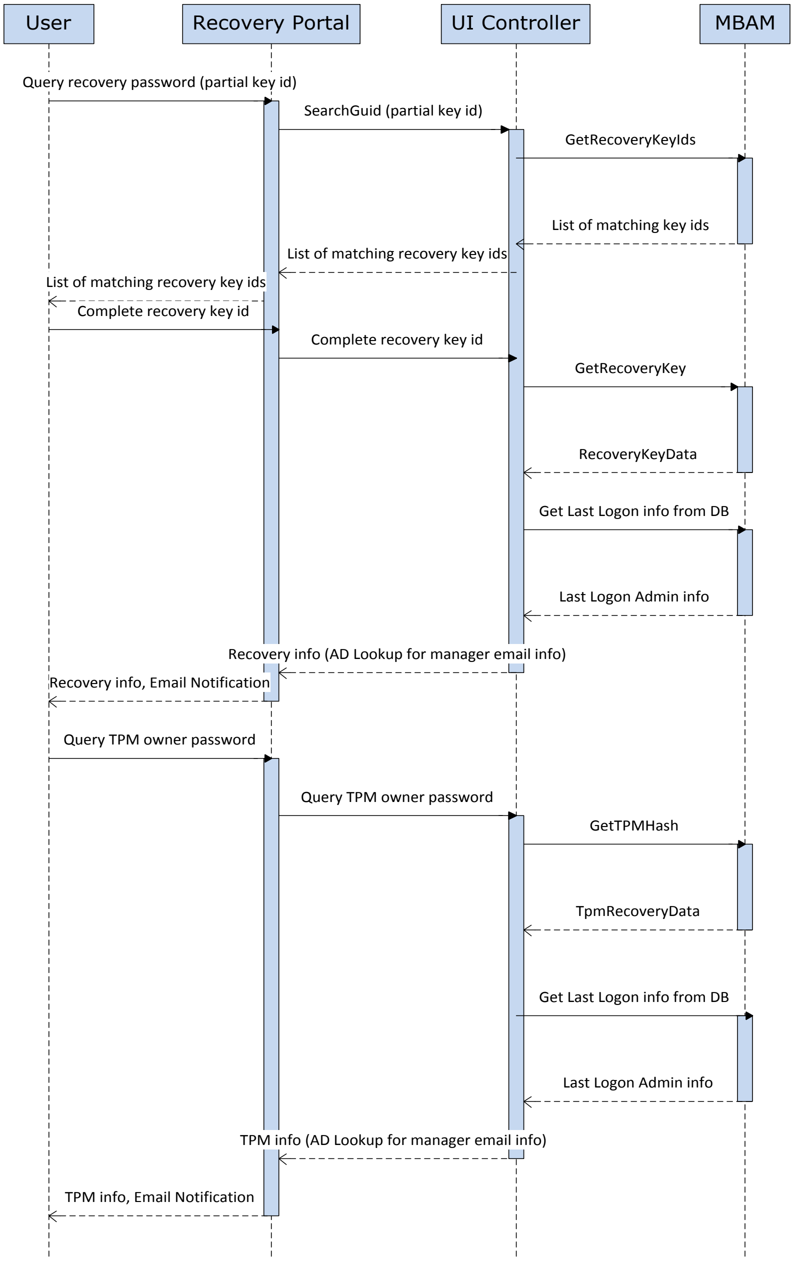
User
Recovery Portal
UI Controller
MBAM
Query recovery password (partial key id)
SearchGuid (partial key id)
GetRecoveryKeyIds
List of matching key ids
List of matching recovery key ids
List of matching recovery key ids
Complete recovery key id
Complete recovery key id
GetRecoveryKey
RecoveryKeyData
Get Last Logon info from DB
Last Logon Admin info
Recovery info (AD Lookup for manager email info)
Recovery info, Email Notification
Query TPM owner password
Query TPM owner password
GetTPMHash
TpmRecoveryData
Get Last Logon info from DB
Last Logon Admin info
TPM info (AD Lookup for manager email info)
TPM info, Email Notification

Figure 4. Recovery Portal with MBAM

CONCLUSION

BitLocker Drive Encryption ensures that corporate data is secure. MBAM adds to the assurance by enabling graceful management of BitLocker encryption on corporate computers. MBAM features reporting functionality, enhances compliance and simplifies provisioning of Bit Locker Drive Encryption. In addition, it stores recovery keys in an encrypted SQL database, and simplifies the recovery of lost keys. This whitepaper provides guidelines for customization of recovery capabilities for your enterprise needs by using the MBAM interfaces and infrastructure provided by MBAM. The Tasmanian Traders example illustrates the scenarios and the workflow of a custom portal using MBAM.

FOR MORE INFORMATION

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information through the World Wide Web, go to:

http://www.microsoft.com

http://www.microsoft.com/technet/itshowcase

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.