SELF SERVICE RESET PASSWORD MANAGEMENT

ARCHITECTURE GUIDE

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

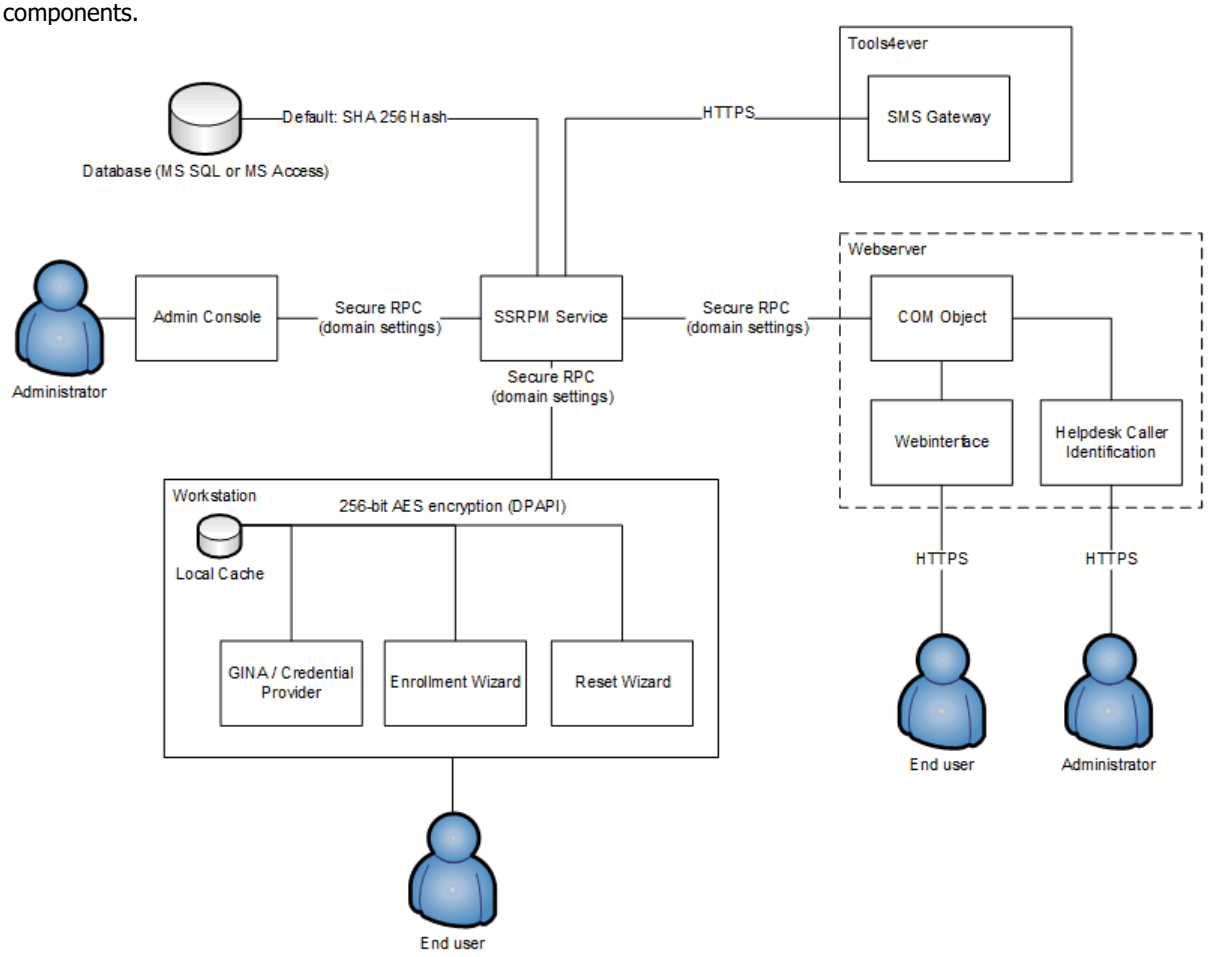
Contents

1. Introduction

SSRPM consists of many components that communicate with one another. Some of these components also store (encrypted) information in a database or in files. This document describes all of the components of SSRPM, what kind of data is stored, the encryption used and the communication methods.

2. Architecture

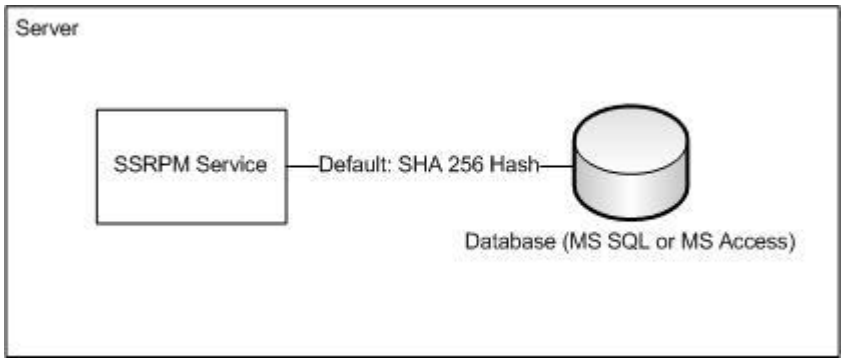
SSRPM consists of multiple components. This chapter describes these components and their relation to other components.



Overview of components and their relation.

2.1. SSRPM Service

The main component of SSRPM is the SSRPM Service. This service manages all of the connections with the clients as well as the connection with the SSRPM Database. The SSRPM Service may be installed on any server in the network. The MSSQL database does not need be be installed on the same machine.



Communication
The SSRPM Service communicates with the SMS Gateway over an HTTPS connection.
By default the SSRPM service communicates over port 39746 with the clients.

Security
The most important data stored by SSRPM service are the user answers. In order to store the data safely and to support certain functionality, the SSRPM service supports the following mechanisms to store the user answers in the database:

- Clear text
- MD5
- SHA 256 (Default)
- Reversible encryption

Clear text
The answers are stored in the database as plain text. This option is not recommended.

MD5 and SHA 256 hash
The answers are stored in the database as a hash. It is not possible to reconstruct the original answer from a hash. It is recommended to use SHA 256 hashing as it is the most secure method.

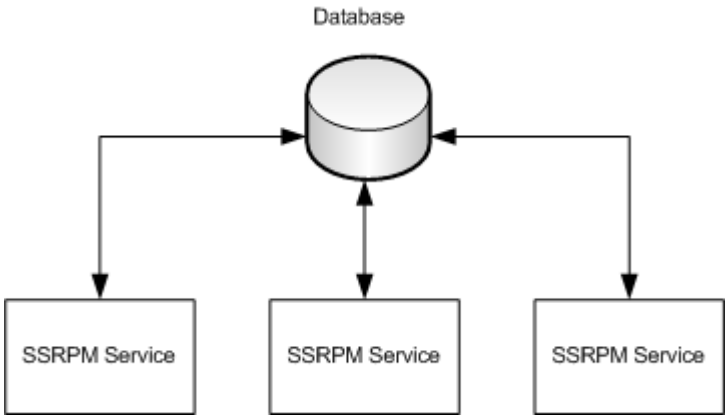
Reversible encryption
The reversible encryption is based on the credentials of the SSRPM service account and uses 256-bit AES encryption. This option is required for the helpdesk caller identification functionality.

2.1.1. Fail Over / Redundancy

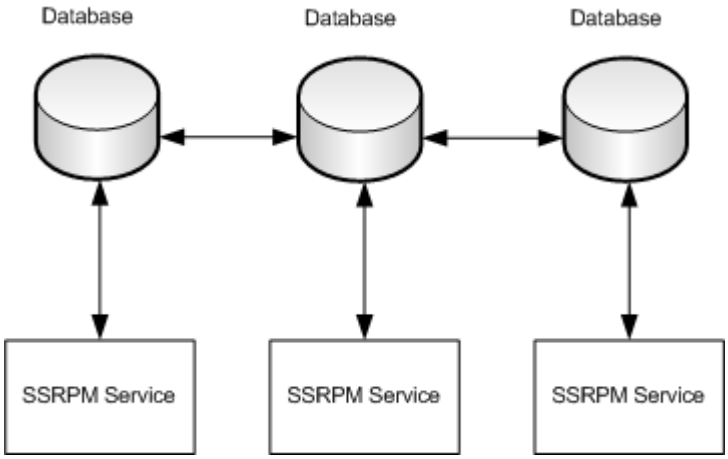
SSPRM is designed so that it can be configured in a high availability situation.There are several mechanisms that may be used to achieve high availability.

Offline mode
The user clients can be configured so that they cache user and configuration data locally on the client machine. This allows users to logon using SSRPM even if the SSRPM service is not available. The functionality provided by the user client offline mode can also be used to service laptops that are not always connected to the company network. When the laptops connect to the network, they communicate with the SSRPM service to exchange data. This data is then stored locally so that the user can continue to use SSRPM when he/she works at home or another location.

Multiple SSRPM Services
Multiple SSRPM services may be installed to provide high availability in case of hardware failure on one of the servers that is running the SSRPM service. The clients will automatically connect to another server if the connection to the SSRPM service fails, assuming the server names are pushed to the clients.



Multiple SSRPM databases
In combination with multiple SSRPM services multiple Databases may be used. The databases must run on a MSSQL server and replicate the data stored in the database to the other SSRPM databases. The configuration guide contains a step by step guide on how to configure an MSSQL server for replication.



2.2. Admin console

Administrators can use the admin console to install and manage the SSRPM service.

Security
The admin console communicates with the SSRPM Service using secure RPC connection. The encryption method used by the secure RPC connection depend on the security settings of the domain. The minimal encryption used is 128 bit RC4 encryption.

2.3. Client software

The client software consists of three components:

1. Enrollment wizard
2. Reset Wizard
3. GINA/Credential Provider

2.3.1. Enrollment Wizard

The enrollment wizard is installed on the workstations. The end user can use this application to enroll in SSRPM. It also checks periodically if a user is enrolled, if the user should re-enroll and (if applicable) if the data in the local cache is up-to-date. The local cache is only used for the offline logon functionality. If this functionality is not enabled, no data stored in the local cache.

Local Cache
The local cache contains all the information required to perform a offline logon. This includes profile and user data. The data stored in the local cache is stored as binary data and is encrypted using the local system account using Windows Data Protection which use 256 bit AES encryption. On top of that, the answers are additionally encrypted with the unencrypted answer or hash as salt. This means that the answers can only be decrypted if you already have the answer.

Security
The enrollment wizard communicates with the SSRPM Service using secure RPC connection. The encryption method used by the secure RPC connection depend on the security settings of the domain. The minimal encryption used is 128 bit RC4 encryption.

2.3.2. Reset Wizard

The reset wizard is installed on the workstations. The end user can use this application to reset his/her password or unlock his/her account.

Local Cache
The local cache contains all the information required to perform a offline logon. If the reset wizard can't connect to the SSRPM service it will look in the local cache if it can perform an offline logon.

Security
The reset wizard communicates with the SSRPM Service using secure RPC connection. The encryption method used by the secure RPC connection depend on the security settings of the domain. The minimal encryption used is 128 bit RC4 encryption.

Offline SMS
If the SMS authentication is enabled and required during the offline logon procedure, the reset wizard will try to connect to the SMS Gateway over an HTTPS connection and the transmitted data will be encrypted using 128 bit RC4 encryption.

2.3.3. GINA/Credential Provider

SSRPM includes two types of GINA's/Credential providers, the standard GINA/Credential provider and the offline GINA/Credential provider.

Standard
The standard GINA/Credential provider is installed on the workstation with the enrollment- and reset wizard. It doesn't use the local cache nor does it communicate with the SSRPM service.

Offline
The offline GINA/Credential provider needs to be installed on the workstation separately, in addition to the client software. It also doesn't communicate with the SSRPM service, but it does cache credentials for the offline logon procedure. The cached credentials are encrypted using 256 bit AES encryption.

2.4. COM Object

The COM object is typically used by the web interfaces of SSRPM.

Security
The COM object communicates with the SSRPM Service using secure RPC connection. The encryption method used by the secure RPC connection depend on the security settings of the domain. The minimal encryption used is 128 bit RC4 encryption.

2.5. Webinterface

It is recommended to install the web interface on a separate server, especially if it can be accessed from outside the network. The end user can use the webinterface to enroll in SSRPM, to reset his password or to unlock his account.

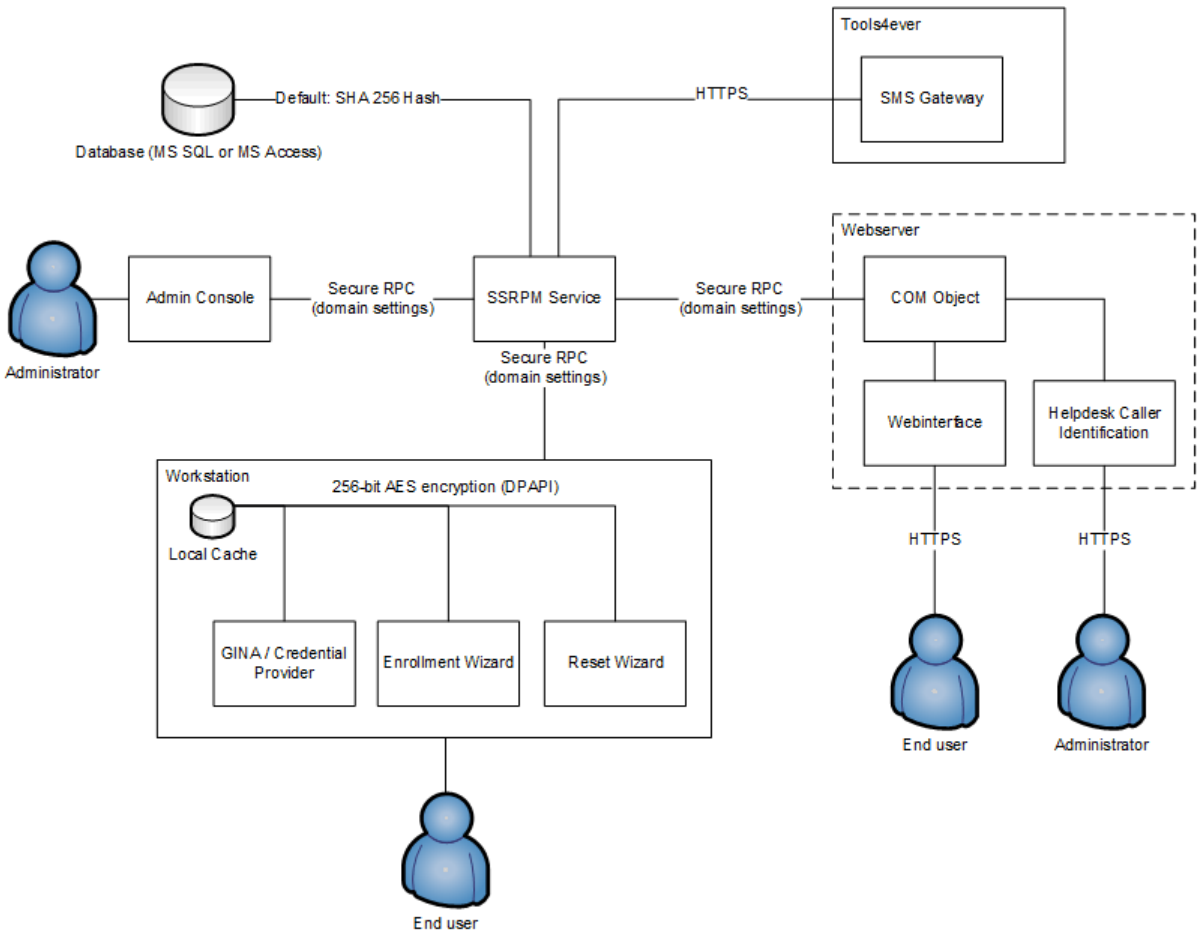
Security
The end user communicates with the webinterface using HTTPS. The webinterface uses the COM-object to communicate with the SSRM Service.

2.6. Helpdesk Caller Identification

The administrator can use this web interface to determine if the end users knows the answers to his challenge questions without finding out the whole answer. This functionality requires that the SSRPM service stores the user's answers using reversible encryption. However the answers are only decrypted by the SSRPM service and never leave the SSRPM service.

Security
The end user communicates with the webinterface using HTTPS. The webinterface uses the COM-object to communicate with the SSRM Service.

2.7. Complete overview



3. Index