Removing MCrypt as a dependency

Mcrypt is no longer used by Tiki since 18.x LTS.

However, it is still used by the SAML feature which depends on php-saml, which is installed by Packages. Upcoming php-saml 3.x will no longer use Mcrypt. Tiki will update to php -saml 3.x as soon as it's released.

The MCrypt component, used in Tiki, is being deprecated.
A new encryption library should be found and implemented. Existing data should be converted.

“

> *The mcrypt extension has been abandonware for nearly a decade now, and was also fairly complex to use. It has therefore been deprecated in favour of OpenSSL, where it will be removed from the core and into PECL in PHP 7.2.*
> *Source: http://php.net/manual/en/migration71.deprecated.php*

Features using MCrypt

lib/phpsec

MCrypt references found in phpsec.crypt.php and phpsec.rand.php
Needs to be investigated more

The phpsec library was removed from Tiki17 and is no longer present. Thus not an issue.

Third party libraries

MCrypt may be used by 3rd party libraries.

3rd part libraries having mcrypt references in the code (thus not necessarily called)
In vendor_bundled/vendor

- adodb
- composer
- paragone
- phpseclib
- zendframework

In vendor_extra

- kaltura

User Encryption

The User Encryption enables secure storing of user data within Tiki. The module can operate in Base64 mode (unsecure) and MCrypt mode.

CryptLib encapsulates MCrypt. Existing data uses MCRYPT_RIJNDAEL_256 and MCRYPT_MODE_CBC encryption
If a new library could read this encryption, it could possibly read existing data. Preliminary investigations indicates that this may not be possible. Thus existing data may need to be read by MCrypt before they are converted to a new encryption type using a different library.

New component
PHP mentions MCrypt has been depreciated in favour of OpenSSL.
Needs to be investigated more

Migrating exiting data
Data is encrypted using the user's plain text password (only available at login time). Thus a decryption + re-encryption is not possible using a system/batch process.

Existing data can be converted as a part of the login process. One after one, as the different users log in. Once a user's data is converted to the new encryption algorithm, the old data can be deleted.

The system must be able to determine which encryption algorithm is used, in order to invoke the correct library.
The current (MCypt) encrypted data is stored in tiki_user_preferences.
Example prefName = dp.MyDomain and dp.MyDomain.usr. All names start with "dp."
A new algorithm can use a different prefix, e.g. "dq.", and thus be able to identify the correct encryption algorithm.

Once the MCrypt library is missing, after a PHP upgrade, non-converted user encrypted data can no longer be decrypted. The data is thus lost and must be re-entered. The system could give some kind of indication about how much MCrypt encrypted data is remaining. The admin can then check the possible damage before a PHP upgrade.

The conversion should probably be run automatically in the background (at login time). It should be transparent to the end user. Thus no user prompting or notices should occur.

MCrypt replaced by OpenSSL in User Encryption

OpenSSL is now used by User Encryption. Existing data is attempted converted at log in time. The conversion requires that the MCrypt module is available

Tiki Check

- ~~tiki-check.php should be amended to say it's no longer used, starting in~~ Tiki18 done: https://sourceforge.net/p/tikiwiki/code/64056

tiki-check is updated. It will now check for the OpenSSL extension. The MCrypt check is still present, but the explanation text has been changed. The Tiki Fitness level for MCrypt is now "info"

- Migrating MCrypt