Storing sensitive data in encrypted cache

fork and edit tutorial (https://github.ibm.com/MFPSamples/DevCenter/tree/master/tutorials/en/foundation/7.1/data/storing-sensitive-data-in-encrypted-cache.html) | report issue (https://github.ibm.com/MFPSamples/DevCenter/issues/new)

Overview

Encrypted cache is a mechanism for storing sensitive data on the client side. Encrypted cache is implemented by using HTML5 web storage technology, which allows data to be saved locally and retrieved on subsequent application use or restart.

The data is encrypted and stored by a combination of a user-provided key and a randomly generated token that is retrieved from the server (key-value pairs), which makes it more secure.

Encrypted cache is like a security deposit box: it remains open until you close it, so it is important to remember to close the cache when you are finished working with it.

Encrypted cache is similar to technologies such as:

- Local web or DOM storage
- Indexed database API
- Cordova API: Storage API or File API
- JSONStore

The following table shows how some features provided by encrypted cache compare with other technologies.

	JSONStore	Encrypted Cache	Local Storage	Indexed DB	Cordova Storage	Cordova File
Android Support	Yes	Yes	Yes	Yes	Yes	Yes
iOS Support	Yes	Yes	Yes	Yes	Yes	Yes
Web	Dev. Only (3)	Yes	Yes	Yes	-	-
Data Encryption (1)	Yes	Yes	-	_	_	_
Maximum Storage	Available space	~ 5 MB	~ 5 MB	> 5 MB	Available space	Available space
Reliable Storage (2)	Yes	-	-	-	Yes	Yes
Adapter Integration (1)	Yes	-	-	-	-	-
Multi User Support (1)	Yes	-	-	-	-	-
Indexing	Yes	-	-	Yes	Yes	-
Type of Storage	JSON Documents	Key – value pairs	Key – value pairs	JSON Documents	Relational (SQL)	Strings

(1): These features are further described in the JSONStore (../jsonstore/) tutorial.
(2): Reliable storage means that your data is not deleted unless the application is removed from the device or one of the methods that removes data is called.
(3): "Dev. Only means that it is designed only for development. There are no security features and a ~5 MB storage space limit.

This tutorial covers the following topics:

- Supported browsers and devices

- Creating and opening encrypted cache
- Reading, writing, and removing data by using encrypted cache
- Closing and destroying encrypted cache
- Changing the encryption key
- Sample application

Supported browsers and devices

You implement encrypted cache by using HTML5 web storage technology.
The following table shows which browsers support web storage for mobile devices.

Show all versions	IE	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	IE Mobile
								2.1		
						3.2		2.2		
						4.0-4.1		2.3		
	8.0					4.2-4.3		3.0		
	9.0		28.0	5.1		5.0-5.1		4.0		
	10.0	23.0	29.0	6.0		6.0-6.1		4.1	7.0	
Current	11.0	24.0	30.0	7.0	17.0	7.0	5.0-7.0	4.2-4.3	10.0	10.0
Near future		25.0	31.0		18.0					

= Supported = Not supported

For more information, see the Can I use (http://caniuse.com) page.

Creating and opening encrypted cache

To create or open previously created encrypted cache, use the following API:

`WL.EncryptedCache.open(credentials, createIfNone, onComplete, onError);`

- `credentials` – A string value that represents a user-provided password.
- `createIfNone` – A Boolean value that specifies whether new encrypted cache is created if none is found.
- `onComplete` – A callback function to be invoked when cache opening/creating is complete.
- `onError` - A callback function to be invoked when cache is not successfully opened/created.

```
WL.EncryptedCache.open(key, true, onOpenComplete, onOpenError);
function onOpenComplete(status){
   busyIndicator.hide();
   alert("Encrypted cache succesfully opened");
}
```

Note: Before you create a new encrypted cache, make sure that the application can connect to the MobileFirst Server instance.

A callback function can receive one of the following statuses:

- `WL.EncryptedCache.OK` – The encrypted cache was successfully opened or created.
- `WL.EncryptedCache.ERROR_CREDENTIALS_MISMATCH` – An attempt was made to open existing

encrypted cache by using wrong credentials.

- `WL.EncryptedCache.ERROR_SECURE_RANDOM_GENERATOR_UNAVAILABLE` – Unable to generate random token due to MobileFirst Server unavailability.
- `WL.EncryptedCache.ERROR_NO_EOC` – Could not open encrypted cache because it was not previously created.
- `WL.EncryptedCache.ERROR_LOCAL_STORAGE_NOT_SUPPORTED` – The device does not support HTML5 local storage.
- `WL.EncryptedCache.ERROR_KEY_CREATION_IN_PROGRESS` – An `open()` or `changeCredentials()` request is already running.

Example

```
WL.EncryptedCache.open(key, true, onOpenComplete, onOpenError);
function onOpenComplete(status){
   busyIndicator.hide();
   alert("Encrypted cache succesfully opened");
}

function onOpenError(status){
   busyIndicator.hide();
   switch(status){
      case WL.EncryptedCache.ERROR_KEY_CREATION_IN_PROGRESS:
         alert("ERROR: KEY CREATION IN PROGRESS");
         break;
      case WL.EncryptedCache.ERROR_LOCAL_STORAGE_NOT_SUPPORTED
:
         alert("ERROR: LOCAL STORAGE NOT SUPPORTED");
         break;
      case WL.EncryptedCache.ERROR_NO_EOC:
         alert("ERROR: NO EOC");
         break;
      case WL.EncryptedCache.ERROR_COULD_NOT_GENERATE_KEY:
         alert("ERROR: COULD NOT GENERATE KEY");
         break;
      case WL.EncryptedCache.ERROR_CREDENTIALS_MISMATCH:
         alert("ERROR: CREDENTIALS MISMATCH");
         break;
      default:
         alert("AN ERROR HAS OCCURED. STATUS :: " + status);
   }
}
```

Reading, writing, and removing data by using encrypted cache

When the encrypted cache is open, operations such as reading, writing, and removing data can be performed.

Storing data

To store data in encrypted cache, use the following API:
`WL.EncryptedCache.write(key, value, onSuccess, onFailure);`

Example

```
WL.EncryptedCache.write(key, value, onWriteSuccess, onWriteFailure);
function onWriteSuccess(status){
    alert("Succesfully encrypted into cache.");
}

function onWriteFailure(status){
    if (status == WL.EncryptedCache.ERROR_EOC_CLOSED)
        alert("Encrypted cache closed, write failed. error code= "+ status);
}
```

Reading data

To read data from the encrypted cache, use the following API: `WL.EncryptedCache.read(key, onSuccess, onFailure);`

Example

```
WL.EncryptedCache.read(key, onDecryptReadSuccess, onDecryptReadFailure);
function onDecryptReadSuccess(value){
    alert("Read success. Retrieved value :: " + key + " = " + value);
}
function onDecryptReadFailure(status){
    alert("Encrypted cache closed, reading failed");
}
```

Removing data

To remove data from the encrypted cache, use the following API:

`WL.EncryptedCache.remove(key, onSuccess, onFailure);`

Example

```
WL.EncryptedCache.remove(key, onRemoveSuccess, onRemoveFailure);
function onRemoveSuccess(status){
    alert("Succesfully removed from cache.");
}
function onRemoveFailure(status){
    alert("Encrypted cache closed, remove failed");
}
```

Closing and destroying encrypted cache

To avoid possible unwanted access to encrypted cache, close it. After an encrypted cache is closed, access to its data is not possible without the encryption key that was used to create it.

To close the encrypted cache, use the following API:

`WL.EncryptedCache.close(onComplete, onFailure);`

Example

```
function destroyCacheClicked(){
    WL.EncryptedCache.destroy(onDestroyCompleteHandler
,
    onDestroyErrorHandler);
}

function onDestroyCompleteHandler(status){
    alert("Encrypted cache destroyed");
}

function onDestroyErrorHandler(status){
    alert("Error destroying Encrypted cache");
}
```

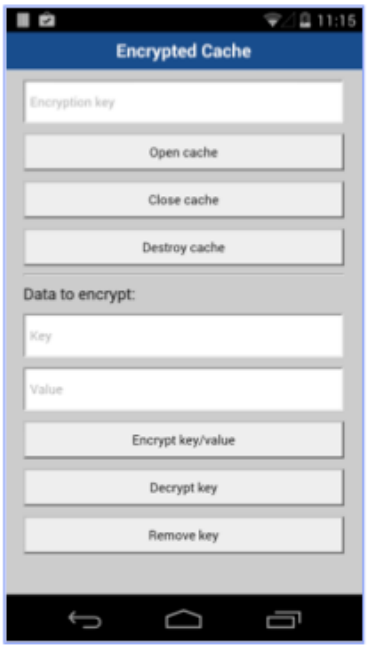
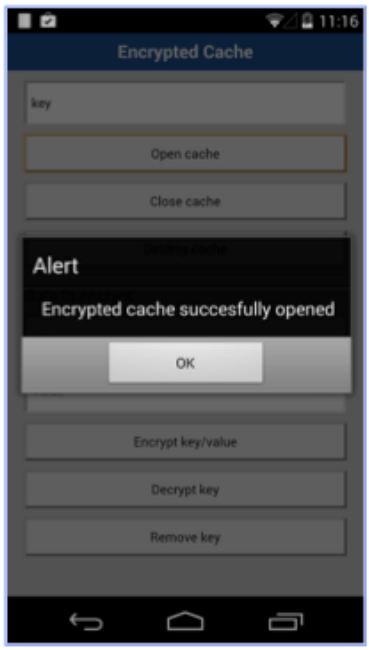
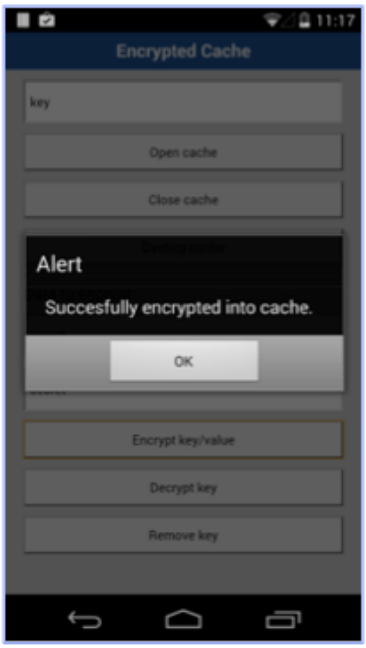
Changing the encryption key

While encrypted cache is in the open state, you can change the encryption key.
To do so, use the following API:

`WL.EncryptedCache.changeCredentials(credentials, onComplete, onError)`

- `credentials` – The new user password to be used.
- `onComplete` – A callback function to be invoked when the change has completed.
- `onError` – A callback function to be invoked in case of an error.

Each parameter is a callback and receives a status object as its response. The available statuses for the `changeCredentials` method are the same as the statuses for the `WL.EncryptedCache.open` method (see Creating and opening encrypted cache).

Sample application

Click to download (https://github.com/MobileFirst-Platform-Developer-Center/EncryptedCache/tree/release71) the MobileFirst project.