W3C Workshop on The Future of Off-line Web Applications - 5 November 2011
Redwood City, CA, USA

Title : Some WebApp offline usecases and requirements, having in mind some security requiring market segments, by Gemalto

Source : Gemalto (Virginie GALINDO)

Abstract : This paper is collecting some drivers, usecases and security requirements, gemalto would like to share with the W3C community, gathered to discuss the future of Offline WebApp. It recommends to take into account the need of security when services are offered to the user offline.

Gemalto is addressing several market segments requiring high security requirements, such as identity area, financial world, corporate market. As a security and innovative concerned company, we would like to prepare the migration of high value or sensitive services toward WebApp technology, and share with W3C community security concerns that our customers may have when doing so.

The migration of all types of services towards a WebApp version is easily predictable due to its well known advantages. The continuity of service, including offline situation will soon become a must have. For services which are offering broadcasting general information to the user, this migration does not require any specific security. But for services relying on end-user credential or end-user private information (e.g. user profile), there is a need to keep a consistent security mechanism when the WebApp is used offline. As an example, in case service provider would like to maintain a minimum of service to the user, an offline security mechanism should replace the online security mechanism.

Some of the following use cases may help to better list some of the security requirements:

Mobile services and public transportation services
NFC public transportation services are usually presented to the end-user thanks to a wallet of services maintained on the device. As an example, a public transportation application can offer the possibility for the end-user to buy travel subscription, but also contextual timetable based on users preference, transportation balance. Sensitive high value information are stored in the secure element (e.g. balance, user profile, …) while other information may be stored and maintained by the wallet on the device. The service provider may want to allow the end-user to access part of the services when being offline.

Corporate - email access
Some WebApp can be used to access corporate mail through personal but controlled device, allowing to view mails in mobility situation. The offline usage of the WebApp may lead to a complete deny of mail access, but in some cases it may be desirable to have access to the latest mails, or latest retrieved documents. In that case, there is a need to maintain a minimum security policy, to make sure that in case the device is lost or stolen, data consultation is protected.

eGovernment services
WebApp are suitable for offering to citizen services to administrate their identity, income declaration, situation changes. In case of offline situation, the government may decide to let

the citizen access some personal and non-sensitive information such as official identifiers.

Mobile banking
WebApp for financial services do require today a strict online management. But one can imagine that a limited set of services may be offered offline, such as latest registered transactions, recent balance, …

For all those security requiring applications, the service provider may want to provide some basic services when being offline. In that case, the following functional security requirements should be envisaged. (This list is not exhaustive but is a suggestion for discussion).

Maintenance of the WebApp trust
The WebApp should have a predictable and reproducible behaviour when being offline, this implies the integrity of the code accessed by the end-user.

Awareness of offline/online context
The WebApp should be able to identify it is in a online or offline context, in order to be able to offer a limited set of functionality to the end-user, if the service provider has decided to. A status related to the availability of online access should be managed by the WebApp.

Offline rights/authorization management
For the offline situation, the WebApp may replace its online security check with an offline security check. In that last case, the WebApp should have an offline security reference/ agent, maintaining the security status, following the service provider's policy.

User privacy and service provider business model
When storing some private and confidential information related to the end-user, or having some value for the service provider (on which he may build his business model), offline information should be stored with confidentiality.

Time related security (time stamping, subscription fees)
When working offline, WebApp offering services valid for a specific period of time, or that should be renewed after a specific amount of time or specific date should be able to rely on a guaranteed time.

As a conclusion, Gemalto would recommend W3C to take into account (and enrich) those security requirements for designing the successful solution of future Offline WebApp, and thus allow security oriented service provider to migrate towards WebApp technology.