Creating Trust in the mGov Era: Derived Credentials Make Mobile Easier and Safer

We all have stories of frustration dealing with public entities while trying to get important documents or official procedures done: long lines, grumpy clerks and just general inefficiency throughout even the simplest inquiries. Fortunately, during the lasts years governmental organizations all around the globe at local and national levels have been switching to a more contemporary approach to serve their citizens: eGov and mGov.

Pushed partially by the United Nations, which has encouraged member states to get online, and by the sharp increase of universal access to smart-phones and internet connections the growth of online government services seems only natural.

Official governmental presence on the internet is virtually total by now, since 2014 all UN member states have websites online. Despite this, a significant amount of these websites provide information only, with no option of transactional services offered. This is gradually changing, with a majority of the countries in the world already offering a wide variety of services online, ranging from payment of taxes and fines and registration of new businesses to renewals and requests of official identifications and driving licenses.

An increasing number of transactional services are designed to be used on mobile devices, this subcategory of eGov, known as mobile government or mGov, allows citizens to interact with governmental institutions using mobile websites and apps.

Regardless of the steady adoption of eGov some factors still deter its growth, with security concerns being the top reason. Recent and quite recurrent scandals like the Equifax breach and the Yahoo! hack diminish the public's trust on the digital management of personal information as a whole, despite of the different ways companies and institutions manage sensitive information.

To tackle down these concerns is one of the major challenges for a universal adoption of eGov. NXP is leading the way on this field thanks to our great expertise in eGov solutions and a vast partner network that enables us to innovate at the fast phase of the sector while maintaining a robust standard of security.

One of the most important innovations developed during the last years are the Derived Credentials, *they are essentially a companion to the credential used in a government-issued electronic ID (eID). To create a derived credential, a government agency starts with a genuine, verified eID. The agency then uses the information associated with that verified electronic ID to generate a credential that can be securely stored on the citizen's portable device.*

Derived Credentials need no additional hardware or software and thus work on a broad variety of mobile devices from all budget levels, the seamless integration of the technology makes the interaction with governmental websites and applications a simple but highly secure transaction.

The adoption of Derived Credentials is an important part of a bigger framework to make eGov a more secure platform: The Mobile ID Architecture, that comprises several mechanisms that guarantee the security of the citizens. If you're interested in getting to know more about how we are making this possible, feel free to take a look at our paper "Creating Trust in the mGov Era".

For questions or more information, feel free to contact:

ABCD ABCD
ABCD@nxp.com