Submission to Smart Event'11 Conferences

TITLE OF THE PRESENTATION:
Privacy Preservation and Low Cost Authentication in Federated Identity Management Systems

PRESENTING AUTHOR DETAILS:
Last Name: BOUZEFRANE
First name: Samia
Email: samia.bouzefrane@cnam.fr
Job title: Associate-Professor
Organisation: Conservatoire National des Arts et Métiers
Country: FRANCE
Postal address: 292 rue Saint Martin - 75141 Paris Cedex 03 - France
Phone number(s): +33 (0)1 40 27 25 83

Last Name: Thoniel
First name: Pascal
Job title: Chairman Executive & CTO
Email: thoniel@ntx-research.com
Organisation: NTX Research
Country: FRANCE
Postal address: 111 avenue Victor Hugo - 75116 Paris - France
Phone number(s): +33 (0)1 46 45 63 93

Last Name: Laurent
First name: Maryline
Email: Maryline.Laurent@it-sudparis.eu
Job title: Professor
Organisation: Télécom SudParis
Country: FRANCE
Postal address: 9 rue Charles Fourier - 91011 Evry - France
Phone number(s): +33 (0)1 60 76 44 42

Last Name: Bekara
First name: Kheira
Email: Kheira.Bekara@it-sudparis.eu
Job title: PhD student
Organisation: Télécom SudParis
Country: FRANCE
Postal address: 9 rue Charles Fourier - 91011 Evry - France
Phone number(s): +33 (0)1 60 76 44 42

CONFERENCE YOU SUBMIT TO: **eSmart Conference**
(remove unwanted items)

ABSTRACT (300-500 words):
With a boom in online services generally accessed through a login/password couple, Internet users have an ever increasing number of digital identities. Indeed, Internet was not originally designed with the digital identity idea and, some solutions have been proposed to deploy digital-identity management architectures using existing standards and protocols such as InfoCard standard that is a user-centric approach or Liberty Alliance standard that is based on the notion of identity federation.

Typical identity management architecture requires basic components like an identity provider (IDP) that authenticates the user in a secure manner allowing him/her to access to a service provider (SP) that provides services and an attribute provider (AP) to supply the user attributes to any authorized

agent while not compromising privacy.

Our presentation tries to bring a solution to some requirements by implementing a comprehensive platform that allows new secure electronic services while ensuring privacy within a transparent and interoperable federated identity management. The requirements are:

- the user must have control on his personal data,
- a great number of certificates must be provided to users with low cost,
- privacy must be preserved, and
- multiple services may belong to distinct spheres and accessible via various material supports like usb key, smart card or a mobile equipment.

In this context, a new PKI-based protocol, called "2.0", has been proposed to guarantee secure access to electronic services at low cost. Based on three levels, PKI 2.0 protocol integrates:

- An international hierarchical PKI that delivers and manages server certificates for identity providers, service providers and attribute providers.
- An internal hierarchical PKI deployed by each registration authority (associated to each circle of trust) for all its agencies.
- A "user" PKI, non hierarchical (without Certification Authorities), that addresses final users.

The first step of our contribution concerns the "user" PKI that integrates an entity called “electronic notary” used instead of a certification authority, allowing the registration of new users (citizen/consumer/professional) within a registration authority that may be a proximity agency (telecom agency, banking agency) viewed as a trust third party. The proposed crypto-system is based on the same principle whatever asymmetric algorithm is used. The local registration authority delivers a "public key certificate" to the user (not signed by a Certification Authority) along with a private key using his usb key, his smart card or his cell phone. The local registration authority also generates and uploads the "public key property certificate" of the user (not signed by a Certification Authority) to its central electronic notary server through a secure channel. Thus, anyone, any IDP, any application and any process can request this electronic notary server to authenticate the digital identity of the user, letting it access at any time services belonging to distinct circles of trust.

The second step occurs after the authentication is completed, and enables the user to automatically preserve his privacy during his electronic transactions by comparing the privacy policy of the SP against his privacy preferences. That is, on one hand, the SP is required to express his policy into our own XPACML language (eXtensible Privacy Access Control Markup Language), i.e. its own list of required/optional data attributes according to their categories, along with the associated P3P basic tags proposed by the P3P platform: Purpose, Recipient, and Retention. On the other hand, the user defines his preference for each of his ID card, for each data category and for each data attribute. According to our newly defined P3P tag classification, upon receiving the SP’s policy at the beginning of the transaction, the user is able to compare the XPACML policy sent by the SP against the preference of the user. In case each unitary negotiation relative to one piece of the policy is successfully done, then the whole negotiation is successful, otherwise, it fails.

KEYWORDS best describing the scope of your presentation (3 or 4)
Public Key Structure (PKI), identity management system, circle of trust, privacy.

Bullet points: **The 3 or 4 key points of your presentation**
They best sum up your presentation and make it appealing to the audience (1 line each max.)
1/ We propose a transparent and interoperable Identity Management platform.
2/ This platform allows to access secure electronic services.
3/ A new non hierarchical “user” PKI 2.0 protocol is proposed allowing low-cost user registration.
4/ A privacy middleware that has been developed enables privacy contract negociations to guarantee privacy.

Short bio (2 or 3 lines) of the author(s)

Samia Bouzefrane is an associate-professor at the CNAM (Paris). She is researcher at CEDRIC Lab and she works on the security of embedded systems and trust systems, on SOA for embedded systems and on how to measure their performance. Particularly, she worked on how to benchmark Java Card platforms. She took part in many ANR projects (MESURE, FC², MURPHY). Since 2008, she is a member of the ACM SIGOPS France board.

Pascal Thoniel holds a Master of Finance from IEP Paris (Sciences Po). After 10 years of experience in Business IT, Pascal has created NTX Research in 1997, a company specialized in Information Systems security. Pascal has 15 years of experience in IT Security : IT Security Audit and Policy designer, inventor XC Technology (strong authentication and confidentiality - patented), inventor of a new user-centric and non-hierarchical approach for PKI (patent pending).

Maryline Laurent is professor at the French National TELECOM SudParis institute. She is the head of the research lab VIS and, member of the French CNRS UMR 5157 SAMOVAR. Her main topics of interest are related to network security, in particular authentication and privacy, mesh/ad hoc networks, RFIDs. In 2009, she co-authored a book "Wireless and Mobile Networks Security" (ISTE). She chaired the International Conference on New Technologies, Mobility and Security, NTMS 2011, Security Track, February 2011.

Kheira Bekara is PhD student in TELECOM SudParis under supervision of Prof. M. Laurent. She is currently working at automating privacy considerations into electronic transactions.

Thank you to send a PHOTO of the speaker ATTACHED to your email.

Submission to be sent to: lperron@strategiestm.com