# A Privacy Preserving E-Payment Architecture

Aude Plateaux[1,2], Vincent Coquet[2], Sylvain Vernois[1], Patrick Lacharme[1],
Kumar Murty[3], and Christophe Rosenberger[1]

[1] ENSICAEN, 17 rue Claude Bloch, 14000 Caen, France
[2] BULL SAS, Avenue Jean Jaurès, 78340 Les Clayes-sous-Bois, France
[3] Department of Mathematics, 40 St. George Street, Toronto, Canada

**Abstract.** This poster proposes a secure e-payment architecture for online shopping protecting users' privacy.

**Introduction.** Online shopping is becoming more and more interesting for customers because of the ease of use and the large choice of products. A vast amount of sensitive information is transferred during such online payment transactions what involves privacy problems. Current e-payment schemes, such as 3D-Secure or the SET protocol, attempt to ensure the actors' security, however, the privacy issues are not addressed in the literature. For instance, when the customer wants to purchase an online service, he/she must provide his/her personal bank information: Personal Authentication Number (PAN), Card Verification Value (CVX2) and expiration date. These secret data are then transferred and can be known by all actors while such knowledge is not necessary.

**Proposition.** In the proposed architecture, private information is only disclosed when necessary and hidden from both the service provider SP, and the payment providers. This solution is mainly based on the generation of two documents: an electronic bank cheque associated with certificates and a contract between the SP and the customer. In this architecture, we conserve two of the three 3D-Secure domains: the acquirer domain and the issuer domain. The interoperability domain is replaced by an interbank trusted third party. This interbank system enables communication between banks without disclosing information about the other actors and without adding any additional message. Moreover, this e-payment architecture is fully compliant with the data minimization, data sovereignty and data sensibility principles. More particularly, the payment transaction never discloses any customer's bank information. Finally, the customer does not need to have particular cryptographic knowledges.

**Conclusion.** While keeping an equivalent level of security, the proposed e-payment architecture is more respectful of the actors' privacy than the ones currently used. This scheme also supports the following properties: the customer's basket, as well as the SP's name, are unknown to the customer's bank. Moreover, the customer does not know the SP's bank and is unknown to this latter. Finally, the customer's banking information and the customer's banks are unknown to the SP.