# The Mobile Java Card™⋆ Grid Project

Serge Chaumette[1], Konstantinos Markantonakis[2]
Keith Mayes[2], and Damien Sauveron[3]

[1] LaBRI, UMR CNRS 5800, Université Bordeaux 1
351 cours de la Libération, 33405 Talence CEDEX, France

[2] Royal Holloway, University of London, Information Security Group-Smart Card Centre⋆⋆
Egham, Surrey, TW20 0EX, United Kingdom

[3] XLIM, UMR CNRS 6172, Université de Limoges
83 rue d'Isle, 87000 Limoges, France

**Abstract.** This position paper presents an overview of the Mobile Java Card Grid project that consists in setting up a grid like mobile infrastructure based on SIM cards. It combines the Java Card Grid infrastructure developed at the LaBRI, the SIM experience and tools of the Royal Holloway University of London, and some features of the MADNESS project developed at the XLIM.

**KEYWORDS**: *Java Card, (U)SIM, JSR177, Java Midlet, GSM/3G, Secure Distributed Environment, Security of Mobile Applications.*

## 1 Introduction

The goal of the Mobile Java Card Grid project is to explore new application domains, by extending to a mobile context based on mobile phones the possibilities offered by the original Java Card Grid [1] developed at the LaBRI by the Distributed Systems and Objects team. The mobile grid will be composed of (U)SIM cards embedded in a set of mobile phones, what makes it possible to achieve this extension still providing the same level of security as in the original platform which is composed of Java Cards,

In this paper we present the main characteristics of the platform, the challenges to solve to achieve its implementation, and the prospective applications that it would make possible to run.

⋆ Java and all Java-based marks are trademarks or registered trademarks of Sun microsystems, Inc. in the United States and other countries. The authors are independent of Sun microsystems, Inc. All other marks are the property of their respective owners.

⋆⋆ The ISG Smart Card Centre was founded in October 2002 by Royal Holloway University of London, Vodafone and Giesecke & Devrient to create a world-wide centre of excellence for training and research in the field of smart cards, tokens, security and applications.

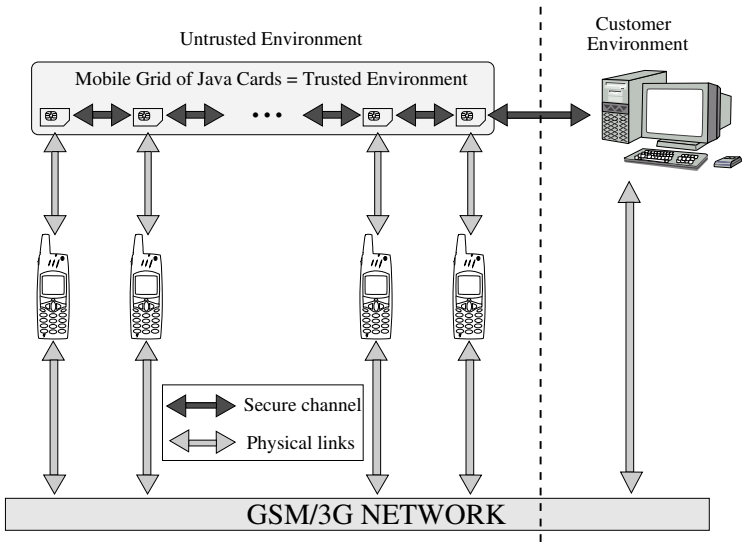


**Fig. 1.** The Mobile Java Card Grid architecture.

## 2 Overview of the Mobile Java Card Grid Framework

In this section we describe the main challenges that have to be dealt with to achieve the Mobile Java Card Grid project.

*Application deployment.* It is already possible today to securely deploy applications Over The Air (OTA) in the (U)SIM cards of mobile terminals, so as to be able to offer a dynamically extensible set of services. Nevertheless, it was shown in [2] that there are practical channel bandwidth constraints in the already deployed GSM networks. Thus, to securely deploy applications in this context, we will use the methods overcoming these problems and presented in [2] or the more suitable protocols and strategies developed at the ISG-SCC as described in [3,4]. All these methods are compliant with the GlobalPlatform [5,6] installation requirements and are thus applicable for already fielded and unprepared devices and cards.

*Communication.* Communication will be supported by the GSM/3G network possibilities (through the Sim ToolKit API – 3GPP TS 43.019 [7]). We will also use the Bluetooth/WiFi connectivity of the smartphones (when available) if the destination of a message can be reached this way. When that kind of communication is used, the Mobile Java Card Grid shares some aspects with the MADNESS (Mobile AD hoc Network with Embedded Secure System) project [8,9] developed at the XLIM.

*Pro-activity.* The (U)SIM cards are really well suited for this project because of their pro-activity. This feature had to be developed specifically for the original Java Card Grid since the Java Cards are passive [10].

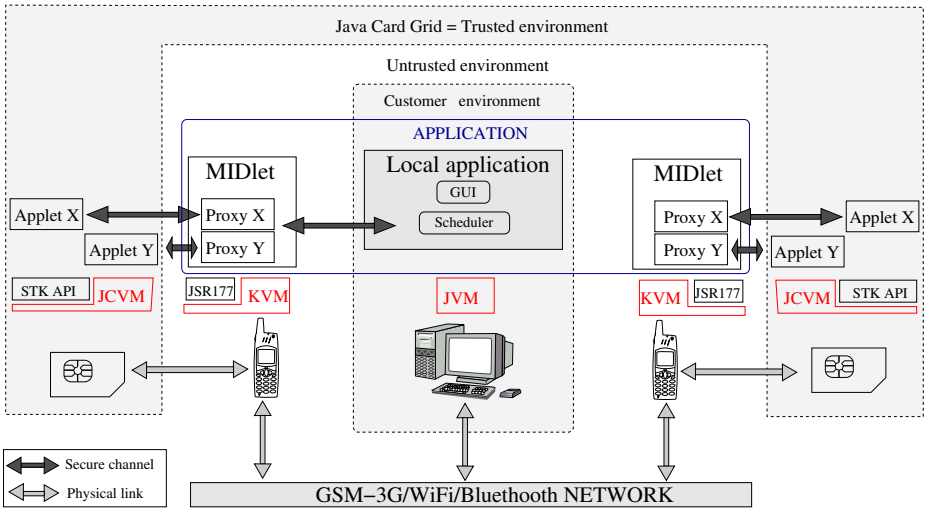


**Fig. 2.** The Mobile Java Card Grid software stack.

*Memory limitation.* Next generation cards will provide 1 Gigabyte of memory. Nevertheless, in order to overcome the memory size restriction of the already fielded SIM cards, we plan to use the solution developed at LaBRI [11,12] that provides smart cards with a secondary storage (*i.e.* the memory of the device or a distant server) which increases the memory capacity for the embedded applications.

## 3 Prospective Applications

A large number of applications can be designed that take advantage of this platform. A straightforward example is a service that would look for a piece of information such as the phone number of a given contact inside the (U)SIM cards of all the employees of a company. Another example is a service that would enable to share the credentials acquired by the members of a group. Furthermore, by locally using the platform in a peer to peer manner, when applicable, it also makes it possible to set up a multilevel ad hoc network, the robustness of which is a key feature to a number of security demanding applications.

## 4 Conclusion

Even thought there is currently no running prototype, we have developed all the blocks to built it in the near future. This will be a joint project between the Royal Holloway, the LaBRI and the XLIM.

## Thanks

The Java Card Grid project at LaBRI is supported by Gemplus, IBM BlueZ Secure Systems, SCM Microsystems, SmartMount and Sun microsystems. We also thank Fujitsu, Giesecke&Devrient, Oberthur Card Systems and Sharp for the Java Card samples. ISG Smart Card Centre participation in this project is thanks to the support of Vodafone and Giesecke & Devrient.

## References

1. Atallah, E., Chaumette, S., Darrigade, F., Karray, A., Sauveron, D.: A Grid of Java Cards to Deal with Security Demanding Applications Domains. In: Proceedings of the 6th International Conference e-Smart05, Nice, France (2005) **e-smart 2005 award for the best innovative technology**.
2. MacDonald, J.A., Sirett, W.G., Mitchell, C.J.: Overcoming channel bandwidth constraints in secure SIM applications. In Sasaki, R., Qing, S., Okamoto, E., Yoshiura, H., eds.: 20th IFIP International Information Security Conference (SEC 2005) - Small Systems Security and Smart cards,. Volume 181 of IFIP International Federation for Information Processing., Springer Science and Business Media (2005) Chiba, Japan.
3. Sirett, W.G., MacDonald, J.A., Mayes, K., Markantonakis, K.: Design, installation & execution of a security agent for mobile stations. In Domingo-Ferrer, J., Posegga, J., Schreckling, D., eds.: Smart Card Research and Advanced Applications - Proceedings of the Seventh IFIP WG 8.8/11.2 International Conference, CARDIS 2006. Volume 3928 of Lecture Notes in Computer Science., Spinger-Verlag (2006) 1–15 Tarragona, CAT, Spain. ISBN: 3-540-33311-8.
4. Sirett, W.G., MacDonald, J.A., Mayes, K., Markantonakis, K.: Secure deployment of applications to fielded devices and smart cards. In Fernández-Medina, E., Yagüe, M.I., eds.: Security in Information Systems - Proceedings of the Fourth International Workshop on Security in Information System (WOSIS 2006), INSTICC Press (2006) 195–206 Paphos, Cyprus. ISBN: 972-8865-52-X.
5. GlobalPlatform: GlobalPlatform. (`http://www.globalplatform.org/`)
6. GlobalPlatform: Card Specification v2.2. `http://www.globalplatform.org/specifications/card/GPCardSpec_v2.2.zip` (2006)
7. 3GPP: Subscriber Identity Module Application Programming Interface (SIM API) for Java Card. Stage 2. `http://www.3gpp.org/ftp/Specs/archive/43_series/43.019/43019-600.zip` (2005)
8. Bonnefoi, P.F., Poulingeas, P., Sauveron, D.: MADNESS: A Framework Proposal for Securing Work in Ad Hoc Networks. In: Proceedings of CCCT'05, Austin, Texas, USA (2005)
9. Atallah, E., Bonnefoi, P.F., Burgod, C., Sauveron, D.: Mobile AD hoc Network with Embedded Secure System. In: Proceedings of the 1st International Conference Ambient Intelligence Developments 2006 (AmI.d2006), Nice, France (2006)
10. Chaumette, S., Karray, A., Sauveron, D.: Secure Collaborative and Distributed Services in the Java Card Grid Platform. In: Proceedings of the 2006 IEEE International Symposium on Collaborative Technologies and Systems (CTS 2006), Workshop on Collaboration and Security (COLSEC'06), Las Vegas, NV, USA (2006) 56–63 ISBN: 0-9785699-0-3.
11. Chaumette, S., Karray, A., Sauveron, D.: The Software Infrastructure of a Java Card Based Security Platform for Distributed Applications. In: Proceedings of the 8th International Conference on Enterprise Information Systems (ICEIS 2006), 4th International Workshop on Security In Information Systems: WOSIS 2006, Paphos, Cyprus (2006)

12. Chaumette, S., Karray, A., Sauveron, D.: Secure Extended Memory for Java Cards. In: Proceedings of he 2006 International Conference on Computational Science and its Applications (ICCSA 2006), Glasgow, UK (2006) (Poster).