Nom du projet :	Sécurité Java Card
Entreprises ou organismes :	SERMA Technologies / LaBRI

Projet Sécurité Java Card

Rapport d'avancement
Phase 2
Novembre 2001 à Septembre 2002

Serge Chaumette, LaBRI
Jean-Pierre Lacoustille, SERMA
Damien Sauveron, SERMA/LaBRI

Résumé

La technologie Java Card occupe 50 % du marché du logiciel pour cartes à puce multi-applicatives, les 50 % restants étant occupés par Multos. A ce jour, cette technologie est surtout utilisée dans le domaine bancaire et dans le domaine du GSM. Son avantage est d'offrir un système ouvert, c'est à dire un système sur lequel de nouvelles applications peuvent être mises en place et les applications résidentes peuvent être mises à jour. La contrepartie de cette souplesse est le risque que l'ajout d'une nouvelle "applet" puisse exposer le produit à des attaques non envisagées au départ. Ce problème de sécurité est le principal obstacle au développement de cette technologie.

C'est dans ce cadre que SERMA Technologies et le LaBRI réalisent en commun le projet intitulé « Sécurité Java Card ». Ce rapport intermédiaire en rappelle le contenu, synthétise les activités menées au cours de sa seconde phase et présente les résultats obtenus.

Ce document est basé sur le rapport d'avancement rédigé à l'issue de la phase 1 du projet.

Nom du projet :	Sécurité Java Card
Entreprises ou organismes :	SERMA Technologies / LaBRI

1 Présentation générale du projet - Rappel

1.1 Objectifs et finalités

L'industrie de la carte à puce prévoit un fort développement du marché des produits Java Card dans les années à venir. Toutefois, la plupart des clients des industriels requièrent aujourd'hui un niveau d'assurance élevé pour la sécurité de ces produits. Pour pouvoir garantir ce niveau de sécurité, les Centres d'Evaluation de la Sécurité des Technologies de l'Information (CESTI) doivent acquérir l'expertise nécessaire.

C'est ainsi que depuis l'année 1999, le CESTI de SERMA Technologies a eu à réaliser des évaluations sécuritaires de niveau faible (EAL1) sur des produits de type Java Card. Dans ce cadre, afin de développer les compétences nécessaires, une première expérience a été menée avec le LaBRI sous la forme d'une formation au langage Java ainsi qu'une courte collaboration pour le développement de nouveaux types d'attaques. Ce premier contact a permis de mettre sur pied une collaboration à plus long terme dans le domaine de Java Card.

Cette collaboration est centrée sur l'analyse de la sécurité de la nouvelle génération de cartes à puce Java Card (sous-ensemble dérivé de Java). Elle a pour but de mettre au point une expertise en défauts de sécurité logiciels sur ces produits. Il s'agit de développer une bonne expertise de la structure des produits répondant aux spécifications Java Card, afin de pouvoir mettre en œuvre une gamme étendue d'attaques logicielles de haut niveau technique permettant de tester et de valider la qualité de l'implémentation des produits sécurisés soumis à une évaluation Critères Communs ou ITSEC.

Au terme du projet, les partenaires prévoient de formaliser les attaques développées sous forme d'un « jeu d'applets agressives » permettant de tester la résistance de divers produits basés sur Java Card à des attaques similaires. En fonction des faiblesses qui auront pu être identifiées, des procédures de vérification systématique de certaines caractéristiques des produits pourront être établies, en collaboration avec la DCSSI (Direction Centrale pour la Sécurité des Systèmes d'Information).

La démarche de ce projet s'inscrit exactement dans le cadre de l'évaluation et de la certification de la sécurité des technologies de l'information, puisque le CESTI de SERMA Technologies est agréé pour réaliser des évaluations sécuritaires de haut niveau.

La réussite du projet contribuera à améliorer la position du schéma français d'évaluation et de certification (représenté par la DCSSI) au niveau national et international, puisqu'il bénéficiera naturellement d'une reconnaissance plus forte lorsqu'un des CESTI agréés disposera d'une compétence pointue reconnue par les industriels pour l'évaluation de la sécurité de ce domaine technologique.

1.2 Partenaires

Partenaire industriel : SERMA Technologies

SERMA Technologies est une société de Services et d'Ingénierie Technologique spécialisée dans le contrôle des composants, systèmes, cartes électroniques et matériaux. La branche électronique est répartie sur les sites de Pessac (siège social), Toulouse, Saint-Egrève et Stuttgart (Allemagne), et compte 120 ingénieurs et techniciens.

Le CESTI (Centre d'Evaluation pour la Sécurité des Technologies de l'Information) est un département de la branche électronique de SERMA Technologies. Ce CESTI, comme tous les centres d'évaluation, est supervisé par l'Organisme de Certification français (DCSSI : Direction Centrale pour la Sécurité des Systèmes d'Information), et réalise des évaluations sécuritaires selon les Critères Communs et les ITSEC, ainsi que des expertises sécurité sur des composants électroniques.

Siège social : 30 Avenue Gustave Eiffel – 33608 PESSAC Cedex

Tél : 05 57 26 08 88 – **Fax :** 05 57 26 08 98

Web : http://www.serma.com/

Contact responsable du projet : Jean-Pierre LACOUSTILLE -
Ingénieur Evaluateur Sécurité

L'activité même du CESTI de SERMA Technologies requiert une veille technologique importante afin de rester de façon permanente à la pointe des nouvelles techniques d'expertise et d'attaque de composants électroniques et des logiciels embarqués. C'est pourquoi dans un but d'amélioration des services fournis, SERMA Technologies investit dans la recherche sur les produits Java Card, pour lesquels un très fort développement est prévu dans les années qui viennent.

Partenaire universitaire : LaBRI

Le LaBRI (Laboratoire Bordelais de Recherche en Informatique) est une Unité Mixte de Recherche (UMR 5800) du CNRS (Département STIC, anciennement SPI) rattachée à l'Université Bordeaux 1 et à l'ENSEIRB.

Ce laboratoire regroupe des chercheurs du CNRS, des enseignants-chercheurs de l'UFR Mathématiques et Informatique et de l'IUT de l'Université Bordeaux 1, de l'ENSEIRB, ainsi que des enseignants-chercheurs de l'Université Montesquieu (Bordeaux 4: Droit et Sciences Economiques) et de l'Université Victor Ségalen (Bordeaux 2 : Médecine et Sciences de la Vie), dont les activités de recherche justifient leur intégration au LaBRI.

Les chercheurs du LaBRI sont répartis en cinq équipes : Combinatoire et algorithmique ; Logiques, langages et applications ; **Modélisation, vérification et test de systèmes informatisés ; Calcul parallèle et distribué ;** Image et son.

Adresse : LaBRI, Université Bordeaux 1

351 Cours de la Libération – 33405 TALENCE

Rattaché à : Université Bordeaux I – ENSEIRB – CNRS

Tél : 05 56 84 69 00 – **Fax** : 05 56 84 66 69

Web : http://labri.u-bordeaux.fr/

Contact responsable du projet : Serge CHAUMETTE – Maître de Conférences

Le LaBRI apporte sa connaissance approfondie du langage Java, celui-ci étant utilisé au sein du laboratoire depuis plusieurs années dans des applications telles que les systèmes distribués. L'objectif est d'appliquer cette expérience de Java à la technologie Java Card et ainsi de parvenir à identifier ses faiblesses potentielles. Cette approche est justifiée par la plus grande antériorité de Java par rapport à Java Card qui n'a que quelques années d'existence. Le LaBRI apporte aussi sa forte compétence en spécifications formelles, indispensable à la modélisation de la spécification Java Card.

2 Programmeinitial de déroulement du projet

2.1 Rappel du programme initial

Nous rappelons ici le programme initial du projet.

Phase 1 (5 mois) : Etapes 0, 1 et 2

Phase 1 (5 mois) : Etapes 0, 1 et 2

Durant cette phase, il s'agit de prendre en main et de développer les outils nécessaires aux travaux de recherches ultérieurs.

Etape 0 : Prise en main de l'outil Java Card par le LaBRI et SERMA Technologies
Etape 1 : Choix d'un microcontrôleur
Etape 2 : Etude et développement d'une machine virtuelle

Phase 2 (5 mois) : Etapes 3 et 4

Dans cette phase l'analyse de la machine virtuelle Java Card doit permettre d'en élaborer un modèle afin de valider les propriétés du système.

Etape 3 : Analyse de la machine virtuelle Java Card
Etape 4 : Elaboration d'un modèle partiel ou complet de Java Card / Spécification formelle

<u>Phase 3 (5 mois)</u> : Etapes 5, 6 et 7

Cette phase consiste à développer des tests d'attaque sur les produits actuels et sur les futures générations de produits.

Etape 5 : Chargement d'applications agressives
Etape 6 : Analyses des futures générations de Java Card dans l'objectif de développer des applications virus.
Etape 7 : Communication et commercialisation

2.2 Planning prévisionnel initial

Le tableau ci-dessous reprend le planning prévisionnel du déroulement des phases du projet, incluant la fourniture de rapports d'activités au terme de chaque phase.

Phases du projet / Mois	**01/01**	**02/01**	**03/01**	**04/01**	**05/01**
Phase 1 : Prise en main et développement des outils nécessaires					
Etape 0 : Prise en main de l'outil Java Card					
Etape 1 : Sélection d'un microcontrôleur	SERMA : fourniture d'un produit permettant de charger une VM Java Card				
Etape 2 : Etude et développement d'une VM Java Card		LaBRI : résultats de l'étude de la VM ou VM développée			
Rédaction et livraison d'un rapport d'activités intermédiaire (R.I.1) pour la phase 1					LaBRI + SERMA : R.I.1

Phases du projet / Mois	**06/01**	**07/01**	**08/01**	**09/01**	**10/01**
Phase 2 : Modélisation					
Etape 3 : Analyse de la VM Java Card	LaBRI + SERMA : premiers tests sur échantillons				
Etape 4 : Modélisation de Java Card / Spécification formelle			LaBRI : modèle formel de Java Card		
Rédaction et livraison du rapport d'activités intermédiaire (R.I.2) pour la phase 2					LaBRI + SERMA : R.I.2

Phases du projet / Mois	**11/01**	**12/01**	**01/02**	**02/02**	**03/02**
Phase 3 : Développement d'attaques logicielles					
Etape 5 : Développement et chargement d'applications agressives	SERMA + LaBRI : jeu d'applications agressives de premier niveau (pas de Verifier embarqué)				
Etape 6 : Nouvelles générations de produits : attaques par applications « virus »				SERMA + LaBRI : jeu d'applications « virus » ou de deuxième niveau (Verifier embarqué)	
Etape 7 : Communication et commercialisation					
Synthèse : rédaction par les partenaires d'un rapport final complet (R.F) des travaux effectués					LaBRI + SERMA : R.F.

3 Bilan et évolution de planning

3.1 Bilan de la phase 1

Un document spécifique dressant le bilan de la phase 1 a été rédigé. La modification de planning qui y avait été indiquée a par la suite été ajustée conformément à l'avenant modifiant la durée du projet et donc sa date de fin.

3.2 Bilan partiel de la phase 2

L'objectif de la phase 2 révisé conformément au planning modifié en fin de phase 1 est le développement de la JVM et sa modélisation partielle.

Etape 2 : Etude et développement d'une VM Java Card

Suite aux études menées en la phase 1, il avait été décidé que le LaBRI développerait une machine virtuelle Java. Cette phase avait été décalée par rapport au planning initial. En effet le recrutement de l'ingénieur prévu dans le cadre du financement du LaBRI n'est effectivement intervenu que le 1er décembre 2001. C'est à cette date que le développement de la machine virtuelle Java a pu démarrer.

Cette machine virtuelle est aujourd'hui terminée pour l'essentiel et des tests ont déjà été réalisés. Cette étape a pris de l'ampleur et des développements vont se poursuivre autour de la plate-forme. En effet, lors de la journée cartes à puces que nous avons organisée - voir plus loin - nous avons senti un intérêt des industriels pour la mise en place d'un projet global autour d'un tel outil. Ces contacts se sont précisés et des réflexions sont donc engagées dans ce sens.

Etape 3 : Analyse de la VM Java Card

Le développement logiciel nous a donné une parfaite connaissance de la machine virtuelle et on peut donc considérer l'étape 3 comme acquise - il reste à rédiger un document de synthèse -.

Etape 4 : Modélisation de Java Card / Spécification formelle

Il s'agit ici de modéliser les parties sensibles de la machine virtuelle Java afin de mieux les comprendre et de mieux comprendre des attaques potentielles.

Cette étape a été décalée. En effet nous avons préféré mettre tout d'abord l'accent sur le développement de l'environnement logiciel. En revanche nous nous sommes pour partie investis plus rapidement que prévu dans certaines étapes de la phase 3 (cf. ci-dessous).

3.3 Activités réalisées dans la phase 3

L'objectif de la phase 3 est le développement d'attaques logicielles et la définition d'une méthodologie pour les réaliser et donc les prévenir. Même si il s'agit en quelques sortes de l'étape ultime du projet, nous avons souhaité l'amorcer avant la fin de la phase 2. En effet ceci nous guide d'une part dans la conception et la réalisation des outils logiciels en cours de développement et d'autre part nous indique les parties sensibles de la machine virtuelle Java embarquée sur lesquelles devra porter l'effort de modélisation.

Etape 5 : Développement et chargement d'applications agressives

Cette phase a été amorcée au travers d'expérimentations menées par Damien Sauveron avec le concours d'Iban Hatchondo. Ces expérimentations nous aident en particulier à définir les fonctionnalités logicielles à intégrer à notre VM afin de supporter la méthodologie de test que nous entendons proposer.

Etape 6 : Nouvelles générations de produits : attaques par applications « virus »

Cette étape n'a pas encore été abordée.

Etape 7 : Communication et commercialisation

Nous avons déjà réalisé une première action de communication. Le LaBRI a en effet organisé une journée intitulée les nouveaux enjeux de la carte à puce le 19 décembre 2001 - cf. plaquette jointe -. Cette manifestation a mobilisé une centaine de personnes qui ont pu à la fois découvrir les technologies, les produits mais aussi les problématiques de sécurité sous-jacentes. Des contacts ont ainsi pu être pris avec les principaux intervenants du secteur (Oberthur, Schlumberger, Gemplus, Sun, etc.). **Il semble que ces contacts puissent conduire à la définition d'une suite au présent projet qui impliquerait tout ou partie de ces intervenants.**

3.4 Planning révisé

Rappelons que du fait des décalages de date dans l'évaluation des propositions et donc des avis émis, on peut considérer que le projet a effectivement débuté mi-juin 2001. Ceci conduit à un décalage de l'ensemble du projet.

De plus la notification de crédits arrivée à l'Université Bordeaux 1 en septembre n'a pas permis de lancer le recrutement de l'ingénieur devant participer au projet dans le temps prévu. Une fois la recherche d'un ingénieur engagée, nous avons pu effectivement recruter Iban Hatchondo le 1er décembre 2001. Ceci a conduit à de nouveaux décalages que nous intégrons à ce planning définitif.

<table>
<tr><th>Phases du projet / Mois</th><th>06/01</th><th>07 et 08/01</th><th>09/01</th><th>10/01</th><th>11/01</th></tr>
<tr><td colspan="6">Phase 1 : Prise en main et développement des outils nécessaires</td></tr>
<tr><td>Etape 0 : Prise en main de l’outil Java Card</td><td>Collecte de la documentation nécessaire (fin DEA Damien SAUVERON)</td><td></td><td></td><td colspan="2">Prise en main des outils Java Card</td></tr>
<tr><td>Etape 1 : Sélection d’un microcontrôleur</td><td></td><td>Décision de travailler sur un environnement d’émulation sur PC.</td><td></td><td></td><td></td></tr>
<tr><td>Etape 2 : Etude et développement d’une VM Java Card</td><td></td><td colspan="4">LaBRI : Etude démarrée – Recrutement ingénieur développement en cours</td></tr>
<tr><td>Rédaction et livraison d’un rapport d’activités intermédiaire (R.I.1) pour la phase 1</td><td></td><td></td><td></td><td></td><td>LaBRI + SERMA : R.I.1</td></tr>
</table>

Le planning de la phase 2 s'est nettement décalé du fait d'une part du recrutement tardif d'Iban Hatchondo et d'autre part de l'importance prise par le développement de la machine Java. Rappelons que nous entendons faire de cet outil le cœur de notre environnement et qu'il pourrait constituer le noyau d'un projet impliquant les différents intervenants industriels du marché de la carte à puce. Les développements vont donc se poursuivre en parallèle avec les travaux de modélisation.

Phases du projet / Mois	**12/01**	**01/02**	**02/02**	**03/02**
Phase 2 : Modélisation (suite)				
Etape 2 : Etude et développement d'une VM Java Card	LaBRI : développement VM			
Etape 3 : Analyse de la VM Java Card	Analyse pour modélisation			
Etape 4 : Modélisation de Java Card / Spécification formelle				
Rédaction et livraison du rapport d'activités intermédiaire (R.I.2) pour la phase 2				
Etape 7 : Communication et commercialisation	Journée cartes à puces			

Phases du projet / Mois	**04/02**	**05/02**	**06/02**	**07/02 et 08/02**	**09/02**
Phase 2 : Modélisation (suite)					
Etape 2 : Etude et développement d'une VM Java Card	LaBRI : développement VM améliorations et outils				
Etape 3 : Analyse de la VM Java Card	Analyse pour modélisation				
Etape 4 : Modélisation de Java Card / Spécification formelle					
Rédaction et livraison du rapport d'activités intermédiaire (R.I.2) pour la phase 2					LaBRI + SERMA : R.I.2

Phases du projet / Mois	**10/02**	**11/02**	**12/02**	**01/03**	**02/03**
Phase 2 : Modélisation (suite)					
Etape 2 : Etude et développement d'une VM Java Card	LaBRI : développement VM - améliorations et outils				
Etape 3 : Analyse de la VM Java Card	Analyse pour modélisation				
Etape 4 : Modélisation de Java Card / Spécification formelle	LaBRI : modèle formel de Java Card				
Rédaction et livraison du rapport d'activités intermédiaire (R.I.2) pour la phase 2					LaBRI + SERMA : R.I.3

Le planning de la phase 3 n'a pas été modifié mais simplement décalé. Notons cependant que l'étape 5 est déjà largement amorcée et que des opérations de communication ont aussi été réalisées (pendant la phase en décembre 2001 - cf. ci-dessus -).

Phases du projet / Mois	**02/03**	**03/03**	**04/03**	**05/03**	**06/03**
Phase 3 : Développement d'attaques logicielles					
Etape 5 : Développement et chargement d'applications agressives	SERMA + LaBRI : jeu d'applications agressives de premier niveau (pas de Verifier embarqué)				
Etape 6 : Nouvelles générations de produits : attaques par applications « virus »				SERMA + LaBRI : jeu d'applications « virus » ou de deuxième niveau (Verifier embarqué)	
Etape 7 : Communication et commercialisation					
Synthèse : rédaction par les partenaires d'un rapport final complet (R.F) des travaux effectués					LaBRI + SERMA : R.F.

Etant donné le décalage important constaté, il convient de faire une demande officielle de modification de calendrier.

4 Conclusion

Ce second rapport permet de cadrer définitivement le projet en terme de déroulement et de calendrier. Les étapes suivantes se dérouleront conformément à la description réalisée dans le présent document.