PKI Consolidation Project and Multiapplicative Smart Payment Cards

Milan Marković¹ · Miloš Kilibrarda¹ · Aleksandar Milošević²

¹Banca Intesa ad Beograd, Security Department
III Bulevar 1c, 11070 Belgrade, Serbia
{milan.markovic | milos.kilibarda}@bancaintesabeograd.com

²Pexim Solutions, Goce Delčeva 44, 11070 Belgrade, Serbia
aca@pexim.co.yu

Abstract

In this paper, main characteristics of the consolidated PKI system in Banca Intesa ad Beograd are described. This PKI system is used for electronic banking services for external users (home banking for physical persons and e-banking for legal persons), as well as a part of the identity management system (windows logon, single sign-on) and other security services for Bank’s internal users (secure e-mail, SSL client authentication). One of the main features of this project is an introduction of the EMV DDA MasterCards in Banca Intesa ad Beograd. These are PKI Multos cards which will have three applications on them: M/Chip Select 4 and CAP payment applications, as well as PKI application. This way, our Maestro users could make payment through POS and ATMs by using the M/Chip payment applications, via Internet in unconnected mode by using external CAP reader and CAP application on the card and, in connected mode, via Bank’s web portal by using the connected smart card reader and PKI application on the card with X.509 digital certificate issued by the consolidated PKI system of Banca Intesa ad Beograd. The PKI consolidated system of Banca Intesa ad Beograd is based on the fully customized domestic PKI solution.

1 Introduction

Banca Intesa ad Beograd has advanced security solutions applied in its banking operations. As many other commercial banks in Serbia (for a survey of a current status of PKI experiences in Serbia, see [Mark04]), Banca Intesa ad Beograd has electronic banking solution for legal persons based on PKI smart cards and digital certificates issued by an in-house PKI solution. By using these e-banking cards, companies could make payment directly online via Bank’s web portal by using a secure web transaction system [SaMa03]. Besides, companies could prepare transactions offline via specialized offline application, sign and encrypt them by using the e-banking card and send them afterwards to specialized web service on the Bank’s side.

Also, Banca Intesa ad Beograd has operated a secure home banking system for physical persons that is currently based on a specific PKI system and specialized mini CD for citizens that stores private asymmetrical key (in encrypted form) and digital certificate. This home banking system is currently based on the out-sourced PKI system. This way, citizens that have registered current account in the Bank, could use these CDs to make signed and encrypted payment transactions via Bank’s web portal through the form of secure web transaction system.

Besides the mentioned PKI systems for external users, Banca Intesa ad Beograd has its own in-house PKI system for internal users (all employees in the Bank) based on smart card USB tokens that store private key and digital certificate. These certificates are integrated into the Windows Active Directory and employees’ USB smart cards are used for Microsoft Windows Logon on the Bank’s Intranet system, as well as for secure e-mail (based on S/MIME protocol) and SSL client authentication for specific web services which are needed for some business operations.

Besides the mentioned e-banking solutions, Banca Intesa ad Beograd is also a leader in payment card operations in Serbia. In the year 2003, Banca Intesa ad Beograd (with a name “Delta banka” in that time) issued a first EMV Visa chip card in Balkan area. Very soon (these days), there will be also start of mass issuing of EMV MasterCard chip cards. These will be Multos 32 K cards with PKI capabilities that include three applications on it: EMV DDA MasterCard payment application, 3D Secure CAP application and PKI application with multiple asymmetrical keypair capabilities. Recently, Banca Intesa ad Beograd also started issuing Amex EMV cards. This way, Banca Intesa ad Beograd is currently 100% in EMV acquiring and issuing for all three brands: Amex (SDA), Visa (SDA) and MasterCard (DDA).

The paper is dedicated to a description of the PKI consolidation project in Banca Intesa ad Beograd which will consist of the unique Root CA and in-house intermediate CA systems for external and internal users. Namely, facing with various issues in dealing with two different PKI systems (current in-house and out-sourced PKI solutions) and introducing new multiapplicative MasterCard EMV DDA chip cards with PKI application and digital certificate on them, Banca Intesa ad Beograd decided to run a PKI consolidation project that will result in an establishment a consolidated and integrated unique in-house PKI solution for both internal and external users. This PKI system will be used also for issuing certificates for SSL servers, as well as for different devices (IPSec enabled routers, firewall, etc.). As a CA software/hardware solution for our PKI consolidated system, we have chosen a Digitrust PKI domestic solution ([Pexi05]) which satisfies all PKI and security international standards, as well as which could be fully customizable to our specific needs and requirements from banking business environment. For example, possible customizations could be related to optimal realization of RSA and standard symmetrical algorithms, according to the results presented in the papers: [UnMD01], [DoUM02], [MaDU02a], [MaDU02b], [MaDU03], [MaDo05], [MaDo06a], [MaDo06b].

The paper is organized as follows. The main characteristics of the PKI consolidation project in Banca Intesa ad Beograd is described in Chapter 2. Chapter 3 is dedicated to brief consideration about multiapplicative smart payment cards. Main characteristics of the implemented PKI solution are listed in Chapters 4-6 while conclusions are given in Chapter 7.

### 2 PKI consolidation Project of Banca Intesa ad Beograd

PKI consolidation Project in Banca Intesa ad Beograd was necessary from the following reasons:

- Establishment of unique in-house PKI solution for all external users – physical and legal persons (home banking and e-banking systems, as well as for some specialized applications like web loans, etc.).
- Using the multiapplicative Maestro EMV smart cards for secure electronic payment of physical persons based on PKI system and electronic signature.