Mecanismos seguros para o auto-aprovisionamento de certificados do Cartão U.Porto

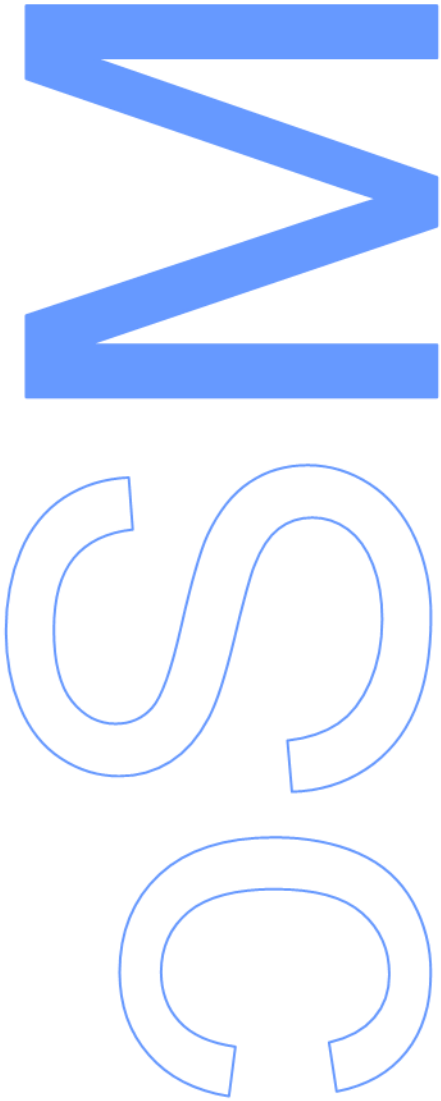
Luís Manuel Magalhães Carvalho Valente Teixeira
Mestrado Integrado em Engenharia de Redes e Sistemas Informáticos
Departamento de Ciência de Computadores
2012

Orientador
Manuel Eduardo Correia, Professor Auxiliar, FCUP

Todas as correções determinadas pelo júri, e só essas, foram efetuadas

.
O Presidente do Júri,

Porto, _____/_____/_____



Agradecimentos

Com breves palavras quero agradecer a todas as pessoas que, de algum modo, contribuíram para a realização deste trabalho:

Aos meus pais, à Margarida, agradeço todo o incentivo e colaboração.

Ao colega e amigo Ricardo Faria, que além do companheirismo, agradeço toda a colaboração e desafio para a implementação de novos serviços com o Cartão U.PORTO.

Agradeço à Doutora Lígia Ribeiro o apoio, incentivo e a facilitação de condições para o desenvolvimento deste projeto.

Ao meu supervisor, Professor Manuel Eduardo Correia, agradeço, para além dos ensinamentos, a disponibilidade e a incitação constante na pesquisa de novas soluções.

Abstract

The University of Porto (U.PORTO) is well aware of the critical institutional role played nowadays by Information and Communication Technologies and is therefore fully committed to obtain and maintain technology leadership for the benefit of its academic community. The U.PORTO smart card identity project is a recent example of a transversal service contribution deployed to enhance student mobility within cam,pus and at the same time increase the sharing of resources and the improvement of the quality of services offered to the academy as a whole. The U.PORTO card is rapidly becoming an indispensable tool in the daily academic life of its users by empowering their access to a growing set of electronic services provided on campus. The outcomes recently obtained by this project, potentiated by other complementary Portuguese Central Government and European initiatives, led DUD (Digital University Department) to focus on the improvement of the cryptographic capabilities of the smart cards currently in possession of its University users, namely, the U.PORTO and the Government issued national e-ID smart cards. The goal of this work is to present the results achieved thus far by the use of the smart cards cryptographic capabilities, particularly, how they can further contribute to the secure dematerialization of several administrative processes, and in the further simplification of the users interaction with the University services.

Resumo

A Universidade do Porto (U. PORTO) ciente do papel crítico desempenhado hoje em dia pelas Tecnologias da Informação e Comunicação está totalmente empenhada em obter e manter a liderança tecnológica em benefício da sua comunidade académica. O projeto Cartão U.PORTO é um exemplo recente do contributo de um serviço transversal implementado que permite fomentar a mobilidade dos estudantes dentro do campus e, ao mesmo tempo, aumentar a partilha de recursos e a melhoria da qualidade dos serviços oferecidos para a academia como um todo. O Cartão U.PORTO tornou-se rapidamente uma ferramenta indispensável no quotidiano académico dos seus utilizadores em grande parte pelo incremento do acesso a um conjunto crescente de serviços eletrónicos fornecidos no campus.

Os resultados obtidos recentemente por este projeto, potenciados em complementaridade por iniciativas do Governo Português e Europeu, conduziram o Departamento para a Universidade Digital em focar-se na melhoria da aplicabilidade das potencialidades criptográficas dos *smart cards* atualmente em posse dos utilizadores da Universidade, nomeadamente, o Cartão U.PORTO e e-ID *smart cards* emitidos por Governos de várias nações.

O objetivo deste trabalho é apresentar os resultados alcançados até ao momento, no potenciar do uso das tecnologias criptográficas, particularmente, no que concerne à implementação de ferramentas criptográficas e como estas podem contribuir para a desmaterialização de diversos processos administrativos, bem como na simplificação da interação dos utilizadores com os serviços da Universidade.

Índice

Lista de ilustrações

Lista de tabelas

Lista de Abreviaturas

AC – Autoridade Credenciadora

AD - Active Directory

API - Application Programming Interface

ATR - Answer To Reset

BST - Banco Santander Totta

CC – Cartão de Cidadão

CNPD – Comissão Nacional de Proteção de Dados

CRL - Certificate Revocation Lists

CSR - Certificate Signing Request

DDA - Dynamic Data Authentication

DH - Diffie-Helman

DNI - Documento Nacional de Identidade

EC – Entidade Certificadora

EEPROM - Electrically-Erasable Programmable Read-Only Memory

EJBCA - Enterprise Java Bean Certificate Authority

EUGridPMA - European Policy Management Authority for Grid Authentication in e-Science

FCCN – Fundação para a Computação Cientifica Nacional

FNMT – Fabrica Nacional da Moeda e Timbre

GNS - Gabinete Nacional de Segurança

HSM - Hardware Security Module

IE - Internet Explorer

IES - Instituições de Ensino Superior

ISO – Normas publicadas pela Organização Internacional para Padronização

JCA - Java Cryptography Architecture

JCE - Java Cryptography Extension

KFUPM - King Fahd University of Petroleum and Minerals

LDAP - Lightweight Directory Access Protocol

NREN - National Research and Education Network

OCSP - Online Certificate Status Protocol

OTP - one-time password

PC/SC - Personal Computer/Smart Card

PED - Pin Entry Device

PEM - Privacy Enhanced Mail

PHP - Hypertext Preprocessor, originalmente Personal Home Page

PKCS - Public-Key Cryptography Standards (PKCS)

PKI - Public-key Infrastructure

RA – Autoridade de Registo

SGBD - Sistema de Gerenciamento de Banco de Dados

SIGARRA - Sistema de Informação para a Gestão Agregada dos Recursos e dos Registos Académicos

SUG – Sistema Universitario de Galicia

TCS - TERENA Certificate Service

TERENA - Trans-European Research and Education Networking Association

TLS - Transport Layer Security

TUI – Tarjeta Universitaria Inteligente

U.PORTO - Universidade do Porto

USC – Universidade de Santiago de Compostela

VA – Autoridade de Validação

VPN - Virtual Private Network

1. Introdução

Esta dissertação apresenta uma solução no âmbito da personalização de *smart cards* com certificados digitais X.509 e discute uma proposta de implementação para o caso concreto do cartão universitário da Universidade do Porto.

1.1. Motivação

Em 2008 a Universidade do Porto (U.PORTO) estabeleceu uma parceria com o Banco Santander Totta (BST) para a emissão do cartão de identificação da comunidade académica. No âmbito desta parceria, a U.PORTO teve acesso a um cartão diferente dos cartões habitualmente utilizados neste género de parcerias. Para além da tradicional componente de identificação visual, incluía como fator inovador, a aglutinação de serviços disponibilizados pela Universidade, potenciando que as tecnologias presentes no cartão fossem utilizadas para disponibilizar uma gama variada de serviços e funcionalidades aos seus utentes. As características deste novo cartão colocariam no horizonte a possibilidade de conceção de um cartão único para utilização no campus, em contraponto com as múltiplas soluções e múltiplos cartões existentes na U.PORTO até então. O novo Cartão U.PORTO (Ilustração 1), foi sendo gradualmente introduzido na vida da universidade e a sua utilização massificada, tornando-se uma realidade no acesso a edifícios, no controlo de assiduidade e no acesso a sistemas de impressão, por exemplo, para além da típica funcionalidade de identificação física e visual.

Ilustração 1- Cartão U.PORTO

Compreendendo a necessidade de inovar, desmaterializar e modernizar processos[1] nos tempos que correm, a U.PORTO tem vindo a adotar medidas que lhe permitam atingir esses objetivos e, nesse sentido, identificou-se como necessária a implementação de um cartão que aglutinasse serviços. A nível nacional, o Estado Português tem fomentado iniciativas semelhantes, por exemplo, através do Cartão de Cidadão (CC) e da Plataforma de Interoperabilidade da Administração Pública[2]. Contudo, na U.PORTO a adoção do CC não era um cenário viável, devido a uma grande comunidade académica estrangeira que não possui CC nem dispõe de documentos de identificação eletrónica. Por outro lado, a associação da identidade civil dos cidadãos a todos os processos e serviços da U.PORTO não seria desejável[3]. Acresce ainda que grande parte dos processos passíveis de desmaterialização são de âmbito interno à organização.

Tal como o projeto Cartão de Cidadão, integrado na política de desenvolvimento científico e tecnológico, o projeto Cartão U. Porto, pretende através da desmaterialização:

- Melhoria da acessibilidade aos serviços públicos, reduzindo barreiras e diversificando os meios de acesso, com menor custo;
- Integração de serviços através da disponibilização de meios e recursos promotores da partilha de dados e informações; da integração de aplicações; da interoperabilidade entre sistemas e da colaboração entre organismos;
- Simplificação de processos e procedimentos administrativos, adaptando-os às exigências de funcionalidade, eficácia e rapidez das novas tecnologias;
- Satisfação das necessidades do cidadão, fornecendo-lhe informação de forma compreensível e útil, eliminando barreiras e obstáculos burocráticos à prestação dos serviços públicos de qualidade;
- Gestão prudente das bases de dados garantindo a sua fidedignidade e segurança, no respeito dos direitos, liberdades e garantias dos cidadãos.

Partindo destes pressupostos, identificou-se a necessidade de proporcionar aos membros da comunidade académica um conjunto de ferramentas que lhes permitissem assinar digitalmente documentos, proceder à autenticação *online* e nos postos de trabalho, bem como garantir a

segurança do transporte de informação através da encriptação de dados, aproveitando preferencialmente o Cartão U.PORTO.

1.2. Cartão U.PORTO

O Cartão U.PORTO é um *smart card*, um dispositivo com capacidade de armazenamento e processamento de informação, com um *chip* de interface dual, colocado sobre cartões de plástico do tamanho tradicional de um cartão de crédito. O *smart card* é um dispositivo seguro, resistente a ataques[4]. A informação armazenada pode ser protegida com segredos partilhados entre o titular do cartão e o chip.

O Cartão U.PORTO tem ainda a particularidade de ser um dos primeiros exemplares de *smart card* com interface dual, isto é, o *chip* do cartão tem uma interface de comunicação que utiliza os seus contactos eletrónicos e uma interface de proximidade que utiliza uma antena. Uma vantagem desta tecnologia reside na capacidade do *chip* do cartão conseguir emular vários protocolos de comunicação de proximidade, expandindo as suas funcionalidades disponíveis. Neste caso concreto, o cartão U.PORTO pode ser utilizado para pagamentos na rede PayPass da Mastercard, com emulação de Mifare[5] e ainda em redes de transportes públicos que utilizem o sistema de bilhética Calypso[6]. Os *smart cards* U.PORTO mais recentes, emitidos após 2010, têm a capacidade de cifrar e decifrar informação.

A emissão do Cartão U.PORTO está assente num procedimento protocolado entre as várias entidades intervenientes no processo, garantido a privacidade dos utilizadores e um compromisso com as políticas de prevenção e segurança da informação. O pedido de emissão de um cartão está dependente da vontade expressa do seu titular, tendo para o efeito que preencher um formulário de pedido do cartão de identificação (Ilustração 2), fornecer a fotografia que deseja utilizar, indicar o nome a inscrever na impressão e o seu número de identificação na U.PORTO. Este formulário é submetido *online*, processo pelo qual o utilizador obtém um documento com os dados de personalização e o número do seu pedido. Na posse deste documento o utilizador dirige-se a um balcão ou quiosque universitário do Banco Santander Totta (BST) para solicitar a validação do pedido. Neste momento, aproveitando o contato com os colaboradores, é feita a identificação do titular do pedido e validada a fotografia submetida. Após a conclusão deste procedimento, os dados de personalização são marcados

como prontos para personalização na Sociedade Interbancária de Serviços (SIBS) Cartões. A ilustração 3, demonstra o processo de pedido e emissão do Cartão U. PORTO.

Ilustração 2- Formulário *online* para pedido de cartão

Paralelamente ao processo de validação realizado pelo BST através da sua rede de balcões, a U.PORTO envia a outra parte do procedimento, nomeadamente um ficheiro totalizador de todos os membros da U.PORTO autorizados a obterem um cartão de identificação, ficheiro que contém a informação para a personalização visual e do chip de contato. Este ficheiro é utilizado para proceder à geração dos ficheiros de produção internos da SIBS Cartões e cruzado com os

dados validados pelo Banco Santander Totta no documento de pedido de cartão. Desta forma, para além de se aproveitar os serviços de validação da identidade das fotografias submetidas pelo BST, garante-se que a produção de um cartão só ocorre para pessoas autorizadas, com base na informação existente no Sistema de Informação para Gestão Agregada dos Recursos e dos Registos Académicos (SIGARRA), ou seja, os estudantes da U.PORTO que se encontrem a frequentar por períodos superiores a 3 meses e os colaboradores ativos com contratos superiores a 3 meses. Complementarmente ao protocolo de emissão do Cartão U.PORTO, o BST e a empresa Gemalto, maior produtor mundial de *smart cards*, fornecem à Universidade o *middleware* necessário para a utilização da componente criptográfica do *smart card*.

Ilustração 3- Procedimento de emissão do Cartão U.PORTO

1.3. Contexto de investigação

De forma a dinamizar a tecnologia criptográfica instalada no cartão, foi disponibilizado, pelo fabricante, à Universidade um *kit* de inicialização, composto por um conjunto de software, leitores e cartões, cujos primeiros testes demonstraram a facilidade de utilização das ferramentas e que a sua integração é compatível com os sistemas utilizados na Universidade. Validada a funcionalidade e a aplicação prática, iniciámos o estudo da operacionalização da personalização criptográfica do Cartão U.PORTO, examinando exemplos de outras universidades nacionais e estrangeiras.

No entanto, comparando o cenário da U.PORTO com outras universidades que já utilizam certificados digitais nos seus cartões universitários, deparamo-nos com várias possibilidades de operacionalização do processo. Se optássemos pela criação de balcões de personalização do Cartão U.PORTO, este processo seria condicionado pela necessidade de afetação de recursos humanos e um espaço específico, que atendendo à realidade de dispersão geográfica das unidades orgânicas da Universidade do Porto na cidade, identificamos como sendo uma solução onerosa.

Outro modelo possível para a personalização criptográfica do Cartão U.PORTO, seria a personalização dos cartões no momento da emissão, junto da SIBS. No entanto, esta solução obrigaria à reemissão de todos os cartões emitidos anteriormente, que à data já ultrapassa mais de 25 mil cartões, e à geração de um certificado assinado por uma entidade certificadora durante o processo de emissão do cartão. Este modelo não parece de fácil implementação por obrigar a desenvolvimentos personalizados pela SIBS Cartões, com custos acrescidos associados, que o parceiro Santander Universidades poderia não aceitar.

Deste estudo, e após diversas reuniões com várias entidades, entre as quais a empresa portuguesa Multicert, acordámos na necessidade de implementar um serviço centrado no utilizador - *user-centric* -, preferencialmente em auto serviço - *self-service* -, de fácil utilização e com elevadas garantias de segurança. A solução encontrada, que usufrui da informação existente no sistema de informação da U.PORTO, é alimentada, em parte, pela informação disponibilizada pela SIBS Cartões após a expedição dos cartões, permitindo identificar e garantir que um cartão pertence a um determinado membro da comunidade académica da U.PORTO, em virtude da informação gravada no chip, durante a personalização.

Estas ações complementam-se na tentativa de procurar resolver o problema de identificação do titular do cartão. Todavia, foi também identificada a necessidade de garantir a autenticidade do utilizador que interage com o sistema, sendo que a primeira possibilidade de solução poderia passar pela utilização da tradicional validação de credenciais, utilizador e palavra-chave, da autenticação do SIGARRA. No entanto, o procedimento de segurança parece pouco robusto para um sistema de valor acrescentado que queremos criar e implementar. Assim, identifica-se como necessário, aumentar os fatores de autenticação do titular do cartão[7].

Analisando as soluções disponíveis para reforçar o mecanismo de autenticação do utilizador, e, acima de tudo, identificada a necessidade de garantir o não repúdio da ação de identificação por parte do titular[8], destaca-se como solução a autenticação com o Cartão de Cidadão. O Estado Português também identificou a necessidade de promover os serviços *online* e para fomentar a modernização administrativa[2] reconheceu a necessidade de fornecer uma identidade digital aos seus cidadãos. O projeto CC, iniciado em 2005, só foi massificado em 2008, e a sua utilização como documento de identificação eletrónica tem aumentado gradualmente, alicerçado na oferta de serviços disponíveis para a utilização do CC, tal como ocorre em outros países europeus.

Convém realçar que o Cartão de Cidadão não foi uma iniciativa tecnológica isolada, tendo sido complementada por legislação que reforça, do ponto de vista jurídico, o valor dos seus certificados digitais. Dessa forma, além das garantias tecnológicas e dos novos serviços que os cartões de identificação eletrónica e os certificados associados permitem disponibilizar aos seus titulares, as suas ações viram o seu valor legal confirmado e validado. Assim, o ato de assinar digitalmente um documento passou a ter o mesmo valor probatório[9] que de uma assinatura em papel realizada pelo seu titular. A autenticação eletrónica realizada através do certificado de autenticação tem o valor de identificação, autenticação e não repúdio da sua realização.

Aproveitando esta nova ferramenta disponibilizada aos cidadãos portugueses, pode-se implementar na U.PORTO uma solução *self-service* que permite ao utilizador autenticar-se perante os sistemas e aplicações com um elevado nível de confiança.

Na posse de soluções para as questões de implementação do serviço, iniciámos a identificação das principais soluções existentes para os certificados digitais. Num primeiro momento, e após

contato com a Multicert, foi ponderado o custo por certificado e o custo de assinatura de uma entidade de certificação raiz, avaliando se estas soluções seriam comportáveis para o cenário global da U.PORTO.

Passámos posteriormente à análise da possibilidade de implementação de uma solução baseada numa entidade certificadora interna à U.PORTO, uma solução cujos custos estavam claramente por calcular na sua plenitude, mas recaindo principalmente em custos de recursos humanos, facilmente realizáveis através das equipas técnicas já existentes. Identificámos também, como mais uma dificuldade, o fator da Autoridade Certificadora (AC) destes certificados não estar contida nas principais distribuições dos sistemas operativos e aplicações em uso, já que os requisitos para fazer parte das listas de autoridades certificadoras são bastante exigentes. Esta circunstância obrigaria a distribuir por todos os membros da U.PORTO o certificado da raiz da autoridade certificadora interna, mas não permitiria retirar proveito da integração elevada já existente ao nível das aplicações, por exemplo, de *office*, para a validação dos certificados digitais utilizados nas operações criptográficas.

A Universidade do Porto mantém uma relação ativa com grupos de trabalho europeus sobre mobilidade de estudantes e desmaterialização administrativa dos processos associados à mobilidade. No âmbito destas reuniões, nas quais participei em representação da U.PORTO, tomei conhecimento da existência de um serviço de certificados pessoais no âmbito do projeto TERENA Certificate Service ao qual Portugal, poderia aderir através da sua representante institucional na organização, a Fundação para a Computação Científica Nacional (FCCN). Desta forma toda a comunidade académica nacional poderia ter acesso a um serviço de certificados pessoais gratuitos, assinados pela Entidade Certificadora (EC) – COMODO. Após analisado o custo deste serviço, que se cifraria num valor fixo anual de 2000 euros, concluímos que, numa perspetiva nacional, seria relativamente reduzido. Esta hipótese pareceu aliciante para o nosso projeto, pois permitiria o acesso a certificados assinados por uma EC raiz a um custo muito baixo, quando comparado com os valores praticados pelas restantes entidades certificadoras comerciais.

Para atingirmos o objetivo de implementação deste serviço, realizámos reuniões com a FCCN a quem apresentámos o projeto da TERENA para Certificados Pessoais e *e-Science*. Os segundos têm enormes vantagens para os utilizadores de redes de computação Grid, uma vez que são acreditados pela European Policy Management Authority for Grid Authentication in e-

Science (EUGridPMA), dando acesso a toda a rede de computação. Foram ainda avaliadas as vantagens de disponibilizarmos às Instituições de Ensino Superior (IES) portuguesas um serviço de certificados pessoais gratuito para o utilizador final e como, dessa forma, poderíamos aumentar e dinamizar a adesão dos utilizadores à assinatura eletrónica e à autenticação *online* com certificado cliente. Dessa forma estaríamos a contribuir para a modernização administrativa das organizações e para o incremento da utilização de ferramentas criptográficas.

Tendo-se verificado a aceitação da nossa proposta, por parte da FCCN, ficou acordado entre as partes que a U.PORTO se responsabilizava pelo suporte financeiro da operação e pela infraestrutura para disponibilização do serviço. A FCCN realizou os contatos institucionais e gere os processos administrativos associados às políticas da entidade certificadora. O serviço foi implementado no âmbito deste projeto de dissertação e está atualmente disponível, sem custos associados, para utilização das IES portuguesas que o desejem.

A solução TERENA permite ter um recurso importante para os certificados pessoais de autenticação e assinatura digital e, desta forma, personalizar os cartões dos utilizadores da U.PORTO com um certificado assinado por uma EC raiz. Contudo, a cifra com estes certificados é um assunto sensível devido à necessidade de *backup* da chave privada do certificado[10], facto que poderia colocar em causa o não repúdio da assinatura digital realizada. Surgiu então a necessidade de implementar uma segunda infraestrutura, dedicada unicamente à componente de cifra, que pode ser apenas uma entidade certificadora interna, uma vez que este tipo de certificados se destina somente a uso pessoal para segurança da informação. Para esta nova infraestrutura identificámos que seria necessário utilizar um sistema de gestão de infraestruturas de chave pública (PKI) que permitisse de forma expedita e profissional gerir o *backup* das chaves e que se integrasse com *hardware* seguro permitindo o *backup* das chaves privadas e oferecendo elevados níveis de confiança aos utilizadores. Após estudo desta problemática, foi selecionada a aplicação *opensource* EJBCA, promovida pela empresa PRIMEKEY. Na escolha do *hardware* foram estudados vários modelos de Hardware Security Module (HSM) e analisados estudos[11, 12] que permitiram identificar um modelo que se revelasse compatível com os objetivos do projeto, o HSM Luna SA 5 da Safenet, pelo qual optamos e adquirimos. No âmbito desta aquisição foi possível frequentar um curso de formação relacionado com a configuração e utilização de equipamentos Luna SA, que permite concluir a

integração do HSM com o EJBCA e, desta forma, tornar-nos capazes de estabelecer uma entidade certificadora para a emissão dos certificados digitais para cifra.

Com a conjugação destas ferramentas, o Cartão U.PORTO poderá ser personalizado através da aplicação desenvolvida no âmbito deste trabalho com dois certificados: um com o par de chaves gerado no *slot*, que impede a extração da chave privada para assinatura digital de documentos e autenticação, assinado pela EC COMODO via serviço TCS da TERENA e outro com o par de chaves importado para o segundo *slot*, para a cifra de documentos. Este *slot* pode ser reescrito, facultando a realização de um backup ou *update* da informação.

O trabalho de pesquisa foi realizado essencialmente nos sítios de referência, utilizando fundamentalmente os termos chave do projeto: *smart card, campus card, pki, university card functionalities.* Os resultados obtidos permitiram recolher boa parte da bibliografia que suporta este trabalho, sendo que a informação disponibilizada pelo fabricante do cartão e do *middleware* também foi utilizada no desenvolvimento das aplicações.

1.4. Comunicações

Dando conta à comunidade académica do progresso do trabalho, foram apresentadas comunicações escritas em diversos eventos, conforme se lista seguidamente:

- Publicadas
    - Valente, L., et al. (2011). User-centric smart card and identity management for the improvement of the electronic services provided by the University of Porto. EUNIS International Congress. Dublin, Irlanda.
- Não Publicadas
    - Valente, L., Faria R. (2012). U.PORTO Campus Card - Opportunities & Challenges. ECCA Conference 2012, Lund, Suécia
    - Valente, L., Faria R. (2012). Cartão U.PORTO Oportunidades e desafios para a Universidade, Workshop Cartão Universitário Inteligente, Universidade do Porto, Portugal

- Valente, L., Faria R. (2012). U.PORTO Campus Card, Taller Trabajo Firma Eletronica - Santander Universidades, Madrid, Espanha

Participação em comissões organizadoras de eventos

- Wokshop Cartão Universitário Inteligente, Universidade do Porto, Faculdade de Ciências, Março de 2012
- European Campus Card Association Conference 2013, Universidade do Porto, Faculdade de Ciências, 26-28 de Maio de 2013

1.5. Estrutura do Documento

No capítulo 2 apresentamos um enquadramento da utilização de cartões de identificação eletrónicos universitários em IES e um resumo do suporte legal que permite implementar a assinatura digital nos processos administrativos da Universidade.

O capítulo 3 apresenta a arquitetura definida para a solução proposta para o problema, aprofundando alguns conceitos tecnológicos importantes sobre *smart cards* que permitiram a implementação da solução.

No capítulo 4 apresentamos a implementação realizada com enfoque para as principais soluções aplicadas aos vários desafios detetados.

O capítulo 5 é dedicado à apresentação da conclusão do trabalho realizado, e do trabalho futuro, apresentaremos ainda alguns exemplos de uso de um Cartão U.PORTO personalizado utilizando a aplicação desenvolvida.

2. Enquadramento tecnológico

2.1. Casos de uso de Cartões universitários

2.1.1. Casos Nacionais

No panorama nacional, existia um projeto de cartão universitário com certificados digitais, na Universidade do Minho, no âmbito da parceria com a Caixa Geral de Depósitos para a emissão do cartão de identificação universitária da instituição. Este processo decorreu durante os últimos 5 anos, tendo sido abandonado no início do ano letivo 2012/2013. Neste caso, os cartões eram personalizados pela SIBS com informação enviada pela universidade e ainda com um certificado digital emitido pela entidade certificadora Multicert. Nas restantes instituições de ensino superior portuguesas, públicas e privadas, não identificámos projetos de operacionalização de cartões universitários com integração de ferramentas criptográficas. No conjunto das IES que aderiram ao cartão fornecido pelo BST, mais de 40 instituições em Portugal, o trabalho desenvolvido nesta área é reduzido. Contudo, várias instituições têm demonstrado interesse em adotar, no futuro, a solução encontrada pelo trabalho realizado no âmbito deste projeto.

Em Portugal verifica-se uma crescente utilização do Cartão de Cidadão como documento de identificação eletrónica[13] para acesso a serviços e assinatura eletrónica de documentos, alvo de desmaterialização administrativa. Ao nível da funcionalidade de autenticação *online,* para além do caso da Universidade do Porto, são conhecidos exemplos no Instituto Superior Técnico, na Universidade do Minho e na Universidade de Coimbra. Ao nível da desmaterialização de documentos é conhecido o exemplo implementado pelo Instituto Politécnico do Porto para assinatura de pautas académicas. A Universidade do Porto e a Universidade de Coimbra também estão a desenvolver projetos de desmaterialização administrativa com recurso ao CC.

2.1.2. Casos Internacionais

No âmbito da parceria com o Banco Santander Totta, estudamos casos implementados em universidades espanholas que utilizam já as potencialidades criptográficas.

A Universidade de Santiago de Compostela (USC) utiliza, desde o ano letivo 2006/2007, a assinatura digital como meio para a desmaterialização do processo de assinatura de pautas académicas. O projeto iniciou-se também através do desafio lançado pela Divisão Global do Santander Universidades, suportada pela evolução legislativa operada pelo Governo Espanhol e pelos normativos aprovados pelo governo regional da Galiza. Numa fase inicial foram realizadas ações para determinar o tipo de assinatura a utilizar, o seu suporte, definição de canais de apoio e desenvolvidos meios de comunicação e formação.

O projeto galego foi separado em 4 momentos distintos, numa fase inicial através do estabelecimento de um projeto-piloto na Faculdade de Direito, duas fases de expansão na Faculdade de Matemáticas e na Escola Universitária de Formação de Professores e, finalmente, a expansão global. Este projeto está ainda num processo evolutivo, sofrendo momentos de avaliação e reengenharia de processos após a conclusão de cada fase da sua implementação. O projeto da USC de assinatura eletrónica e desmaterialização administrativa contempla a utilização dos certificados do DNI eletrónico e dos certificados emitidos pela Fábrica Nacional de Moneda y Timbre (FNMT) suportados pela Tarxeta Universitaria de Identidade (TUI) da USC para a assinatura digital de documentos, principalmente das pautas de avaliação académica.

A FNMT é uma Entidade Certificadora, que lidera o projeto Certificación Española (CERES) para a emissão de certificados digitais, encontrando-se credenciada pela Autoridade Credenciadora (AC) espanhola e fazendo parte da respetiva Trusted-Service Status List.

No caso espanhol, foram identificados, como principais requisitos para a implementação do projeto, a prestação de formação aos membros da universidade e a existência de balcões de atendimento onde se realiza a entrega dos certificados pessoais para o TUI. De forma a dinamizar a obtenção do DNI eletrónico pelos docentes, a USC estabeleceu um protocolo com a Policia Nacional e promoveu sessões de pedido do DNI eletrónico nas suas próprias instalações. Para fomentar o sucesso do projeto são descritos como fundamentais, o apoio da Secretaría Xeral da USC e da Área de Tecnoloxías da Información e das Comunicacións

(ATIC). Paralelamente, foi dado o máximo apoio ao nível do suporte de *software* e *hardware*. Com o desenvolvimento da primeira fase do projeto de assinatura digital focado na administração eletrónica, foram eliminados os trâmites de assinatura física em documentos dos serviços centrais da USC. As pautas foram assim migrando para o novo procedimento e, desta forma, as notas foram imputadas imediatamente ao expediente académico dos estudantes.

O software utilizado pela USC foi desenvolvido em parceria com a empresa espanhola ACOTEC. Este desenvolvimento contemplou a aplicação informática para a personalização dos cartões com os certificados digitais e a disponibilização de uma biblioteca PKCS#11[14] para utilização do cartão.

Mais recentemente, a USC aproveitou os desenvolvimentos realizados no âmbito da assinatura digital, para promover a troca de expediente entre as universidades do SUG – Sistema Universitário da Galiza. Desta forma a Universidade da Corunha, Universidade de Vigo e USC criaram entre si uma plataforma para troca de dados, principalmente ao nível de dados académicos. Outras Universidades espanholas, tais como a de Murcia[15], a de Cádiz[16] e a de Almería[17], já utilizam a tecnologia de identificação eletrónica, tendo, para o efeito, criado regulamentos internos próprios, que regulam a utilização de assinatura digital.

Outro caso estudado[18] foi o da King Fahd University of Petroleum and Minerals (KFUPM), que implementou um cartão universitário baseado num *smart card*, com o intuito de simplificar e melhorar o acesso aos serviços pelos utilizadores em qualquer lugar e em qualquer altura. Neste momento a KFUPM tem já implementado um conjunto de funcionalidades que vão desde o acesso a bibliotecas, controlo de acessos aos edifícios, porta-moedas eletrónico, acesso a serviços recreativos, serviços médicos, acesso lógico a computadores, *e-learning* e internet. No futuro, está previsto suportar mais aplicações, como a proteção à base de dados e a votação eletrónica para os estudantes.

Outro caso a que demos atenção é o do Campus Card System[19], implementado nas universidades chinesas. Trata-se de um sistema de informação desenvolvido ao longo de 10 anos que permite integrar, todos os passos do ciclo de vida do cartão e a sua integração com sistemas e funcionalidades das universidades.

Alguns estudos[20] avaliaram a satisfação dos estudantes com a introdução da tecnologia *smart cards* nos campi. M. Arami, M. Koller e R. Krimmer, aplicaram um questionário[21] a

estudantes universitários, sobre se os cartões universitários deveriam ser utilizados para simplificar procedimentos administrativos e mais de 88% expressaram a sua satisfação pelo cartão ser multifuncional. Segundo o mesmo estudo, os serviços seguintes com mais votação relacionam-se com a autenticação em exames *online*, com a votação eletrónica e com a sua utilização nas máquinas de venda automática.

Um outro estudo[22], incidindo nas principais funcionalidades existentes com *smart cards* em *smart campus* de universidades de quatro continentes, permite concluir que os serviços tipicamente disponíveis englobam a identificação visual, o acesso a bibliotecas e o empréstimo de livros, a utilização de máquinas de fotocópias, o controlo de acesso a espaços físicos e a utilização de porta-moedas eletrónicos.

Na comunidade de instituições de ensino superior, assiste-se a uma discussão[23] abrangente sobre a necessidade de estabelecimento de *standards* e mecanismos de interoperabilidade entre os diversos cartões académicos. Esta necessidade de estabelecimento de protocolos comuns é entendida como uma forma de potenciar a troca de informação em formato eletrónico entre as IES, principalmente ao nível do processo académico, podendo tornar-se num facilitador do acesso de alunos em mobilidade, nas universidades parceiras.

2.2. Sistemas Gestão de PKI

Inerente à implementação de funcionalidades criptográficas no cartão universitário, estão os certificados digitais associados, os quais deverão, preferencialmente, ser geridos através de uma infraestrutura de gestão de chave pública. A utilização de uma aplicação de gestão de PKI torna-se assim vital na implementação de um projeto de emissão de certificados digitais, como o caso do nosso projeto. Aliado ao fator que verificamos, estarmos perante um projeto com um universo significativamente vasto de cartões e certificados a gerir, tornando-se importante estudar as soluções disponíveis para gestão dos certificados a emitir para o Cartão U.PORTO. No mercado existem algumas aplicações para gestão e administração de infraestruturas de chave pública e, no âmbito deste projeto, foi analisada a Microsoft PKI[24] e a EJBCA[25]. A primeira faz parte do sistema operativo Windows Server e permite personalizar e gerar certificados, incluindo dispositivos de hardware como um *smart card*. Inicialmente utilizamos esta aplicação para agilizar o teste do Kit Classic Client fornecido pela Gemalto.

Após a adição da ferramenta ao sistema operativo, a sua integração com o sistema e com os utilizadores existentes é imediata, possibilitando no momento a geração de certificados, a sua revogação e a publicação de serviços de informação do estado dos certificados emitidos como CRL[26] e OCSP[27]. Como é uma aplicação desenvolvida para ambientes empresariais que utilizem MS Windows, a integração com os sistemas operativos clientes é bastante aprofundada, sendo bastante simples disponibilizar certificados para autenticação em postos de trabalho e permitir que sejam importados para *smart cards*. A aplicação permite que o processo de *enrollment* seja realizado a partir de três opções: a) diretamente na consola de gestão de certificados do sistema operativo; b) por políticas de domínio que são utilizadas no momento de autenticação do utilizador ou c) via portal *web* que pode ser acedido pelo utilizador e autenticado através das suas credenciais Active Directory (AD).

Com esta aplicação pudemos realizar os primeiros testes de autenticação de utilizadores em postos de trabalho Windows através do Cartão U.PORTO com um certificado digital, tendo sido ainda possível realizar o teste dos primeiros mecanismos de *auto-enrollment* por parte do titular do cartão. Verificaram-se, porém, alguns contratempos: O primeiro foi a limitação a plataformas Microsoft, sendo que a U.PORTO quer manter as suas escolhas tecnológicas o mais independes possível. Outro inconveniente identificado foi a não existência de plataforma para a gestão e personalização do código PIN do utilizador e PIN administrativo. Verificou-se ainda

que para aceder ao serviço, mesmo que assente no serviço web, a autenticação do utilizador teria de ser realizada perante uma AD e preferencialmente utilizando o *browser* Internet Explorer.

Outros fatores não negligenciáveis incluem os custos de licenciamento e os fatores de autenticação, dado que a aplicação só permite a autenticação com utilizador e *password*, não podendo ser elevados os níveis de autenticação. Na expectativa de ultrapassar as dificuldades identificadas com a aplicação Microsoft PKI, iniciámos o estudo da aplicação *open source* EJBCA. Esta é uma aplicação desenvolvida pela empresa PrimeKey e é utilizada na gestão de PKI[28] como, por exemplo, a do Cartão de Cidadão. A aplicação EJBCA permite a gestão de várias entidades certificadoras, sendo, neste caso concreto, suficiente para gerir uma Entidade Certificadora para a U.PORTO. Ao nível da integração, verificámos que a mesma possibilita a integração com aplicações cliente via API ou *web services*. Além destas interfaces, a própria aplicação fornece uma interface *web* para a gestão e para os utilizadores solicitarem e gerirem os seus certificados.

O EJBCA corre sobre os principais servidores web aplicacionais, sendo essencialmente desenvolvido em JAVA. Ao nível de repositórios de dados, interage com vários sistemas de gestão de bases de dados (SGBD) e ainda com serviços de diretório Lightweight Directory Access Protocol (LDAP). No contexto da U.PORTO, verifica-se que é facilmente integrável com o sistema de informação, pois são suportadas as tecnologias de base de dados Oracle e é integrável com o LDAP, que serve de base ao sistema de autenticação e autorização. Como aplicação especializada na gestão de PKI, o EJBCA dispõe de suporte para diversos Hardware Secure Modules (HSM) com bastante informação, facilitando a sua configuração e integração. A aplicação foi instalada e configurada segundo os tutoriais disponíveis no sítio da Primekey, informação que foi também utilizada para testar o *deploy* de certificados para o Cartão U.PORTO no âmbito de uma entidade certificadora interna à U.PORTO.

2.3. HSM Hardware Secure Modules

No âmbito deste projeto de trabalho, identificámos a necessidade de disponibilizar uma ferramenta que permita aos docentes e investigadores da U.PORTO protegerem a sua informação e os seus trabalhos, utilizando a cifra para o efeito. Um dos principais fatores condicionantes da cifra de informação relaciona-se com a possibilidade de perda e uso indevido das chaves por terceiros, o que, a acontecer, coloca em causa toda a informação cifrada. Esta condicionante coloca um sério entrave à utilização da cifra e é mesmo uma das principais resistências identificadas pelos potenciais utilizadores. Daqui surge a necessidade de criar mecanismos de *backup* da chave privada e garantir inequivocamente a segurança de algo tão importante e privado.

É neste contexto que os HSM surgem como resposta para repositório desta informação. A sua arquitetura de funcionamento, as regras implementadas e as certificações de segurança que contém, permitem criar um serviço de *backup* das chaves privadas de elevada confiança e nos quais os membros de uma determinada PKI confiam. Além das funções de custódia de chaves, os HSM são também utilizados como aceleradores criptográficos, permitindo o *off load* destas operações de *software* para *hardware* criptográfico, com desempenhos bastante superiores.

No estudo da solução a adotar, começámos por contatar os representantes dos HSM suportados pelo EJBCA[29] que estivessem equipados com capacidade de armazenamento de múltiplas chaves criptográficas. Neste sentido foram identificadas duas empresas, a Safenet e a Thales[11]. Ambas as empresas foram contatadas com o intuito de conhecer melhor os seus produtos, tendo sido obtida resposta unicamente da Safenet. Das várias soluções disponíveis neste fabricante, foi considerado como equipamento que se enquadra no objetivo deste trabalho, o HSM LUNA SA 5, pois demonstrou ser o modelo mais versátil, disponibilizando a possibilidade de ser utilizado por várias aplicações e sistemas em simultâneo, ser o modelo com maior capacidade de expansão de memória para os fins identificados, possibilitando ainda a criação de múltiplas partições permitindo segmentar o espaço de armazenamento de chaves. Na tabela 1, podemos verificar os principais perfis de gestão do HSM Luna SA 5. Este, é um HSM com aceleração criptográfica suportando mais de 6 000 operações com chaves 1024-bit RSA por segundo, o modelo adquirido dispõe de espaço de memória para 20 000 objetos criptográficos com chaves de 2048 bit e permite particionar o espaço disponível em 10 partições. Para permitir este espaço de armazenamento tivemos que optar pelo modelo *rack*

mount chassis. Ao nível de segurança o LUNA SA 5 está certificado pelas certificações FIPS *level* 3 e Common Criteria EAL4+ com 3 níveis de segurança. É um *hardware* resistente a ataques, que obriga a autenticação multi-pessoa e de duplo fator através das suas chaves PED - Pin Entry Device. Este conjunto de chaves PED contém uma chave associada a um código PIN que só o seu titular poderá conhecer. Estes *tokens* PED de autenticação existem para os vários perfis inerentes à sua utilização e interação com o HSM.

Tabela 1- Principais perfis de gestão do HSM Luna SA 5

Token PED	Perfil Operacional	Função
	Security Officer	Configuração HSM Definição políticas segurança Criação de partições
	Security Domain	Controla/Define segurança de domínio *Backup* e replicação de chaves
	User Activation	Ativação de partições Geração de chaves, assinatura, encriptação
	Remote PED Auth	Seguração no acesso lógico remoto através de dispositivos de entrada de PIN.
	Tamper Recovery	Recuperação após *tamper* Transporte Seguro

De forma a facilitar a sua administração e gestão foi ainda contemplado no conjunto o Remote SA PED, isto é, o terminal que permite estabelecer uma sessão remota segura com o HSM, mantendo o esquema de autenticação dos utilizadores e perfis através das chaves PED. A aquisição contemplou também um Remote Backup HSM que permite realizar cópias de segurança do HSM LUNA SA 5 de forma remota, utilizando para os mecanismos de segurança do LUNA. Como o HSM LUNA SA 5 é um equipamento único, por enquanto, optamos por

contratar ainda cinco anos de suporte em regime 24x7, com substituição do equipamento por um novo no horizonte de até 24horas.

O HSM LUNA SA 5, para além de poder ser expandido com mais unidades, permite a configuração de um modelo de *disaster recover*, o balanceamento de carga ou mesmo a criação de *cluster* de HSM. Cumulativamente, permite o *offloading* das funções criptográficas realizadas por vários sistemas, retirando vantagem da utilização de criptoprocessadores para a execução de centenas de operações criptográficas por segundo e dos seus criptocontentores para a custódia segura de chaves criptográficas. Este *offloading* poderá ser reutilizado por outras aplicações, por exemplo, pela base de dados do SIGARRA para a assinatura digital ou cifra de informação, a assinatura digital de *logs* dos sistemas e para aplicações de emissão de selo temporal para a assinatura digital de documentos.

No âmbito do processo de aquisição do equipamento, o parceiro Multicert, realizou uma ação de formação interna abrangendo todos os pormenores da operação do equipamento, o que permitiu identificar a existência de uma componente procedimental muito importante, consistindo na definição dos processos e procedimentos e a sua assunção pelos operadores, o que permite criar um conjunto de garantias e separação de papéis não habituais nas organizações.

2.4. Transport Layer Security – TLS

O protocolo Transport Layer Security (TLS) é constituído por duas camadas (Tabela 2 – Camadas do Protocolo TLS), sendo a camada inferior a TLS Record Protocol, que assegura a privacidade e a *reliabiltiy* das conexões e é utilizada para encapsular o protocolo de alto nível, como o TLS *Handshake Protocol*. Este, por sua vez, proporciona segurança na conexão, o que permite garantir a autenticação das partes, utilizando criptografia de chave pública e a negociação de segredos partilhados de forma segura e confiável.

Tabela 2- Camadas do protocolo TLS

Handshake Protocol	**ChangeCipherSpec Protocol**	**Alert Protocol**	**Application Protocol**
Record Protocol			

Quando o TLS é utilizado para proteger comunicações cliente-servidor, na maioria das situações, o *Handshake Protocol* só realiza a autenticação do servidor. Durante a autenticação o servidor envia o seu certificado para o cliente. Por sua vez, o cliente valida o certificado e extrai a chave pública, utilizando-a depois para cifrar a chave de sessão que será utilizada na comunicação futura. No entanto, para serviços que necessitem de autenticação do cliente, o protocolo TLS permite a sua autenticação durante a fase de *Handshake Protocol*. O servidor pode enviar um *Certificate Request,* que requer do cliente o envio do seu certificado, e um *Certificate Verify* para o servidor. O servidor pode autenticar o cliente validando o certificado obtido e utilizando a chave pública desse certificado para verificar a assinatura contida na mensagem do *Cliente Verify*. A autenticação do cliente no TLS requer a existência de uma chave privada e de um certificado no lado cliente. A sua segurança é garantida pela segurança da chave privada. Para atingir níveis elevados de segurança e mobilidade, a chave privada e o certificado para autenticação podem ser armazenados em *smart card* com coprocessadores criptográficos, uma vez que o cartão pode gerar a assinatura digital para a mensagem *Certificate Verify on-card*, e, desta forma, a chave privada nunca sai da área segura de armazenamento do *smart card*.

2.5. Diffie-Hellman

O algoritmo Diffie-Hellman é um algoritmo de troca de chave que pode ser utilizado para o estabelecimento de uma chave secreta, utilizada habitualmente como uma chave simétrica, não sendo utilizado para cifra ou assinatura de informação, mas permitindo o estabelecimento de uma chave partilhada. A segurança do DH baseia-se na dificuldade computacional do problema do logaritmo discreto. A configuração matemática do DH é relativamente simples: um valor p primo e g o gerador, de tal forma que podemos afirmar que para qualquer $x \in \{1,2,\dots,p-1\}$podemos encontrar um expoente n tal que $x = g^n mod\ p$.

Os valores p e o gerador g são públicos para a troca de chave, Alice gera o seu expoente secreto a e o Bob gera expoente secreto b. Alice envia $g^a mod\ p$ para o Bob que por sua vez envia $g^b mod\ p$ à Alice.

De seguida ambos calculam, a Alice $(g^b)^a\ mod\ p = g^{ab}\ mod\ p$

e o Bob $(g^a)^b\ mod\ p = g^{ab}\ mod\ p$

Como resultado é obtido o segredo partilhado, que tipicamente é utilizado como uma chave simétrica.

2.6. Aplication Protocol Data Units (APDU)

Os APDU são utilizados para a troca de informação entre o *host* e o *smart card*, definido na ISO 7816-4[30] que normaliza dois tipos de APDU: instruções de comando, que são enviadas das aplicações externas para o cartão *smart card* e instruções de resposta, que são enviadas do *smart card* em resposta aos comandos. Existem diversas variantes de comandos APDU, no entanto, cada instrução contém:

- Um *class byte* (CLA) que identifica a instrução
- Um *byte* instrução (INS) que determina o comando
- Dois parâmetros P1 e P2 que são utilizados para passar parâmetros ao comando
- Um *byte Length command* (Lc) que especifica o comprimento de dados a serem enviados na instrução APDU.

Dados opcionais:

- Um *byte Length expected* (Le), especificando o comprimento da informação prevista no APDU de resposta. Se o comprimento estiver definido 0x00, o lado *host* espera que seja retornada toda a informação disponível na resposta ao comando.

Os constituintes CLA, INS, P1 e P2 constituem o cabeçalho do Comando APDU (Tabela 3). Tendo o cabeçalho este formato rígido, o corpo da instrução é constituído pelo Lc Data field e Le, podendo tomar várias formas, conforme definido na norma ISO. Na tabela 3, podemos verificar como é constituído o comando APDU.

Tabela 3 – Comando APDU

Comando APDU						
Cabeçalho (requerido)				**Corpo (opcional)**		
CLA	INS	P1	P2	Lc	Data Field	Le

A instrução APDU de resposta (Tabela 4), contém:

- Dados opcionais;
- Duas palavras de *bytes* SW1 SW2, que contém a informação de estado definido na ISO 7816-4.

O comprimento dos dados opcionais da instrução de resposta APDU é o especificado no comando APDU, devendo ocorrer um erro quando o comprimento não for coincidente. O valor de SW1 e SW2 para sucesso na execução da instrução é 0X9000.

Tabela 4 – Resposta APDU

Resposta APDU		
Corpo (opcional)	**Trailer (requerido)**	
Data Field	SW1	SW2

2.7. Cartão U.PORTO

O Cartão U.PORTO, produzido pela Gemalto, pertence à família de cartões Optelio Contactless D32 R5 for Santander, certificados para ambientes bancários pela MasterCard Certification for PayPass - M/Chip4 and M/Chip2.1. Dispõe de um coprocessador criptográfico para criptografia de chave pública e Dynamic Data Authentication (DDA), contem 32k de memória EEPROM disponível para aplicações e dados. Ao nível do *software* o sistema base é Java versão 2.2.1. Ao nível das interfaces de comunicação, dispõe de duas: proximidade e contacto. Sendo um cartão recente, tem tecnologia dual, isto é, o mesmo chip tem as duas interfaces, a interface de contacto cumpre a norma ISO 7816[31] seguindo o protocolo T0. A interface de proximidade é compatível com a norma ISO 14443 -2, -3 e -4 [32-34] e o protocolo de comunicação T=CL Tipo A, operando na frequência de 13,56 MHz, disponibiliza um Mifare de 4K emulado.

Relativamente à componente criptográfica, suporta DES/3DES, RSA até 2048 bits e SHA-1.
Ao nível de aplicações instaladas,

- PayPass M/Chip4 (Mastercard)
  Applet baseada na última versão das especificações MASTERCARD Paypass M/Chip V1.3.

- VSDC2.7.1 (Visa)
  Applet desenvolvida pela VISA cumprindo com as últimas especificações VISA *payment contactless* 2.0.2. Incluindo aplicações VSDC *contactless*, qVSDC and MSD.

- DualVSDC (Visa)
  Applet desenvolvida pela Gemalto na última versão da VISA payment contactless specifications 2.0.2. Incluindo aplicações VSDC *contactless*, qVSDC and MSD.

- Classic IAS V3 (GemSAFE) (PKCS#11 PKI application), ilustração 4
  Esta *applet* permite autenticação forte, assinatura digital e cifra, permite ainda o armazenamento de certificados digitais. A *applet* cumpre o *standard* PKCS#15[35] e

todas aplicações de PKI que usem API's PKCS#11 APIs e/ou Microsoft CAPI pode ser utilizado com a Classic IAS *applet*.

Esta *applet* funciona apenas através do interface de contato.

- WG10

  A Gemalto personalize os cartões com a *applet* WG10 em uso pelo Banco Santander.

- Welcome Realtime (WRT) XLS V7 (Xena)

  Applet para utilização em programas de fidelização de clientes desenvolvida pela WRT.

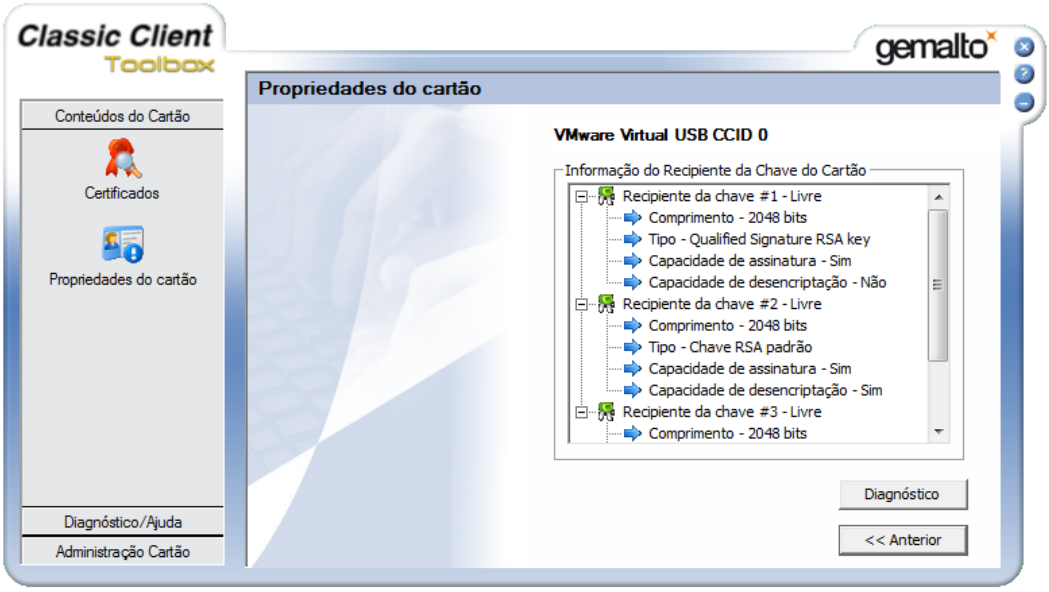


Ilustração 4 - Cartão U.PORTO – criptocontentores

3. Enquadramento legal

3.1. Certificados Qualificados

No estudo das soluções de certificados disponíveis, foi identificada a hipótese de utilização de certificados qualificados. Para melhor compreender o que são, aprofundamos um estudo sobre a legislação em vigor relativamente ao tema. O termo "Certificado Qualificado" foi introduzido pela Comunidade Europeia através da Diretiva 1999/93/CE[36] de 13 de Dezembro de 1999, referindo-se a um tipo específico de certificados para assinatura eletrónica, de acordo com a legislação europeia. Estes certificados são utilizados para a identificação de uma pessoa com um nível bastante elevado de confiança. Os Certificados Qualificados, conforme imposto pela legislação, devem conter pelo menos o seguinte conjunto de requisitos:

- Indicação de que é emitido como um certificado qualificado;
- Identificação da Entidade Certificadora (nome e assinatura eletrónica qualificada) e o país onde está estabelecida;
- Nome ou pseudónimo do titular do certificado e outros elementos que permitam a sua identificação inequívoca. Se existirem poderes de representação, deverá estar indicado o nome do representante ou representantes habilitados, ou um pseudónimo distintivo do titular da assinatura, claramente identificado como tal;
- Chave pública correspondente à chave privada detida pelo titular;
- Número de série do certificado;
- Data de início e data de fim da validade do certificado;
- Identificação dos algoritmos utilizados para a verificação das assinaturas do titular e da entidade certificadora;
- Indicações das restrições a que o certificado está admitido e indicação dos limites do valor das transações para as quais o certificado é válido;
- Indicação dos limites convencionados de responsabilidade da entidade certificadora, sem prejuízo do disposto na legislação em vigor;

- Possibilidade de referência das qualidades específicas do titular, de acordo com as funções a que está destinado o certificado.

No entanto, o cumprimento destes requisitos não é suficiente para que o certificado seja considerado qualificado. Segundo a legislação, o Decreto-Lei n.º 62/2003, que visa compatibilizar o regime jurídico da assinatura digital estabelecido no Decreto-Lei n.º 290-D/99, de 2 de Agosto, com a Diretiva n.º 1999/93/CE, do Parlamento Europeu e do Conselho Europeu, de 13 de Dezembro, relativa a um quadro legal comunitário para as assinaturas eletrónicas, a entidade certificadora também tem que cumprir um conjunto de requisitos aplicáveis aos prestadores de serviços de certificação que emitem certificados qualificados.

Assim, os prestadores de serviços de certificação devem:

- Demonstrar a fiabilidade necessária para a prestação de serviços de certificação;
- Assegurar o funcionamento de um serviço de reportório rápido e seguro e de um serviço de anulação seguro e imediato;
- Assegurar com precisão a possibilidade de verificação da data e hora de emissão ou anulação de cada certificado;
- Verificar, através dos meios adequados e de acordo com a legislação nacional, a identidade e, se for caso disso, os atributos específicos da entidade ou pessoa singular ou coletiva à qual é emitido um certificado qualificado;
- Empregar recursos humanos que possuam os conhecimentos, experiência e qualificações necessária s para os serviços prestados, nomeadamente competência em matéria de gestão e das tecnologias de assinaturas eletrónicas, bem como familiaridade com os processos de segurança adequados; devem ainda saber aplicar processos administrativos e de gestão que sejam adequados e correspondam a normas reconhecidas;
- Utilizar sistemas e produtos fiáveis que estejam protegidos contra modificações e que garantam a segurança técnica e criptográfica dos processos para os quais estejam previstos;

- Tomar medidas contra a falsificação de certificados e, nos casos em que o prestador de serviços de certificação gere dados de criação de assinaturas, garantir a confidencialidade durante o processo de criação desses dados;

- Ser dotados de recursos financeiros suficientes para atuarem de acordo com os requisitos constantes da presente diretiva, nomeadamente para assumirem os riscos decorrentes da responsabilidade por danos, por exemplo através de uma apólice de seguro adequada;

- Registar todas as informações relevantes, relativas a um certificado qualificado durante um período de tempo adequado, nomeadamente para fornecer elementos de prova de certificação para efeitos processuais. Este registo poderá ser feito eletronicamente;

- Não armazenar ou copiar dados de criação de assinaturas da pessoa a quem o prestador de serviços de certificação tenha oferecido serviços de gestão de chaves;

- Antes de iniciar uma relação contratual com uma pessoa que deseje obter um certificado para a sua assinatura eletrónica, informar essa pessoa, através de meios duráveis de comunicação, dos termos e condições exatos de utilização do certificado, incluindo eventuais limitações à utilização deste, da existência de um regime de acreditação facultativa e dos processos de apresentação de queixas e de resolução de litígios. Essas informações devem ser apresentadas por escrito, podendo ser transmitidas por meios eletrónicos, e devem utilizar uma linguagem facilmente compreensível. O pedido destes, deverão igualmente ser facultadas a terceiros que confiem no certificado, elementos relevantes desta informação;

- Utilizar sistemas fiáveis de armazenagem dos certificados num formato verificável, de modo a que:

    - Apenas as pessoas autorizadas possam introduzir dados e alterações,

    - A autenticidade das informações possa ser verificada,

    - Os certificados só possam ser consultados pelo público nos casos em que tenha sido obtido o consentimento do detentor do certificado, e

- Quaisquer alterações de carácter técnico suscetíveis de prejudicar esses requisitos de segurança sejam imediatamente visíveis pelo operador.

3.2. Valor Probatório da Assinatura Eletrónica

A legislação vigente confere a documentos eletrónicos, valor probatório, sendo que no caso português esse valor é definido no Artigo 3.º do Decreto-Lei 290-D/1999, de 2 de Agosto, com as alterações introduzidas pelo Decreto-Lei 62/2003, de 3 de Abril.

- O documento eletrónico satisfaz o requisito legal de forma escrita quando o seu conteúdo seja suscetível de representação como declaração escrita.
- Quando lhe seja aposta uma assinatura eletrónica qualificada certificada por uma entidade certificadora credenciada, o documento eletrónico com o conteúdo referido no número anterior tem a força probatória de documento particular assinado, nos termos do artigo 376.º do Código Civil.
- Quando lhe seja aposta uma assinatura eletrónica qualificada certificada por uma entidade certificadora credenciada, o documento eletrónico cujo conteúdo não seja suscetível de representação como declaração escrita tem a força probatória prevista no artigo 368.º do Código Civil e no artigo 167.º do Código de Processo Penal.
- O disposto nos números anteriores não obsta à utilização de outro meio de comprovação da autoria e integridade de documentos eletrónicos, incluindo outras modalidades de assinatura eletrónica, desde que tal meio seja adotado pelas partes, ao abrigo de válida convenção sobre prova ou seja aceite pela pessoa a quem for oposto o documento.
- Sem prejuízo do disposto no número anterior, o valor probatório dos documentos eletrónicos aos quais não seja aposta uma assinatura eletrónica qualificada certificada por uma entidade certificadora credenciada, é apreciado nos termos gerais de direito. O disposto na legislação portuguesa e europeia não nega os efeitos legais e de admissibilidade como meio de prova para efeitos processuais da assinatura eletrónica, pelo facto de:
    - Não se apresentar pela forma eletrónica;
    - Não ser baseada num certificado qualificado;

- Não ser baseada num certificado qualificado emitido por uma entidade certificadora acreditada;
- Não ter sido criada através de um dispositivo seguro de criação de assinaturas.

3.3. Assinatura eletrónica na U.PORTO

3.3.1. Utilização do Cartão do Cidadão

Os membros da comunidade académica da Universidade do Porto poderão utilizar o seu Cartão do Cidadão para a assinatura eletrónica qualificada de documentos da Universidade. Contudo, o certificado qualificado para assinatura eletrónica presente no Cartão do Cidadão dispõe apenas do nome e número de identificação civil do titular. No caso de existirem poderes de representação e delegação de competências, essas informações não estão contidas no certificado qualificado, conforme indica a legislação vigente. No certificado qualificado também não constam informações sobre a organização a que pertence o titular do certificado, o seu vínculo, categorias ou outras informações sobre a entidade a qual está vinculado.

No Artigo 5.º do Decreto-Lei 290-D/1999, de 2 de Agosto, com as alterações introduzidas pelo Decreto-Lei 62/2003, de 3 de Abril, sobre documentos eletrónicos dos organismos públicos, indica que os mesmos podem emitir documentos eletrónicos com aposição de assinatura eletrónica qualificada, sendo que os dados relativos sobre o organismo e a pessoa que praticou o ato administrativo devem estar indicados de forma a ser facilmente comprovada e identificada a função ou cargo desempenhado pela pessoa signatário do documento. Como no caso de pessoas coletivas a legislação coloca nas Entidades Certificadoras a responsabilidade pela verificação se a assinatura garante a intervenção das pessoas singulares que, estatutariamente ou legalmente, representam a pessoa coletiva, e isto, não ocorre com o Cartão do Cidadão, terá que ser avaliado juridicamente o valor probatório da assinatura de um documento da U. PORTO utilizando o Cartão do Cidadão.

3.3.2. Utilização do Cartão U.PORTO

A aquisição de certificados qualificados não é suficiente para permitir à Universidade do PORTO disponibilizar sistemas de assinatura eletrónica qualificada, visto o atual Cartão U.PORTO não ser certificado (qcSSCD – *qualified certificate Secure Signature Creation Device*). Se a opção recair nos certificados avançados, estes só permitem assinatura eletrónica avançada, o que também está enquadrada na legislação em vigor. O Artigo 3.º do Decreto-Lei 290-D/1999, de 2 de Agosto, com as alterações introduzidas pelo Decreto-Lei 62/2003, de 3 de Abril, nos pontos 4 e 5, permite o estabelecimento de um acordo entre partes para a utilização de outras modalidades de assinatura desde que, ao abrigo de uma convenção válida. Este artigo regulamentar coloca ainda a apreciação do valor probatório da assinatura nos termos gerais do direito para outros tipos de assinatura que não a qualificada.

Ficam, deste modo, patentes várias condicionantes à utilização da assinatura eletrónica e demonstra-se a necessidade de acautelar algumas situações legais, de acordo com os normativos nacionais e europeus. Para cumprir estas orientações, estamos a realizar um levantamento exaustivo dos vários processos e documentos em que se poderá aplicar assinatura eletrónica, bem como a identificação dos intervenientes e respetivas funções. Só desta forma será possível avaliar a necessidade de certificados (qualificados ou avançados) a utilizar na U.PORTO. Apesar de algumas dificuldades na disponibilização de certificados qualificados, a U.PORTO poderá utilizar certificados avançados internamente para assinatura de documentos, desde que estabeleça convenções sobre a prova com as diversas partes.

Perante este quadro e considerando que nem toda a comunidade académica tem, para já, o Cartão do Cidadão, a Universidade quer potenciar o acesso à assinatura eletrónica através do Cartão U.PORTO tanto por utilizadores nacionais como estrangeiros.

4. Implementação

4.1. Arquitetura

A solução desenvolvida assenta numa aplicação cliente e numa aplicação servidor. A aplicação cliente está desprovida de segredos e informação confidencial, mas dispõe de ferramentas criptográficas que lhe permitem estabelecer uma sessão segura com a aplicação servidor. Desta forma, é possível receber a informação necessária para validar o cartão universitário apresentado e realizar a sua personalização.

Na fase inicial da execução da aplicação cliente, utilizámos o protocolo Transport Layer Security (TLS)[37], sucessor do SSL 3.0. O principal objetivo do TLS é proporcionar privacidade e integridade da informação na troca de mensagens entre duas partes comunicantes sobre uma rede não confiável como, por exemplo, a *Internet*. Adicionalmente o TLS permite a autenticação mútua das partes comunicantes.

Nesta fase inicial, a aplicação cliente estabelece uma sessão TLS com a aplicação servidor, requerendo ao utilizador que se autentique na sessão utilizando um certificado digital. Neste caso, utiliza-se o certificado de autenticação do Cartão de Cidadão, sendo o servidor aplicacional o responsável pela autenticação do utilizador e permitindo apenas o acesso de utilizadores autorizados à aplicação. A aplicação servidor irá utilizar o certificado recebido para verificar na base de dados se o pedido é originado por um utilizador válido e existente nos registos. A base de dados contém informação sobre os cartões emitidos, esta informação é fornecida pela SIBS Cartões após a expedição de cada cartão, através da disponibilização via WebDav[38] de um ficheiro contendo os dados utilizados na personalização de cada cartão, permitindo estabelecer uma relação entre o cartão e o seu titular. O acesso ao servidor da SIBS para obtenção dos ficheiros de expedição é realizado através do protocolo Webdav sobre uma conexão HTTPS com credenciais utilizador e palavra passe para autenticação e filtragem do IP cliente.

Após a autenticação do utilizador, e se a mesma for válida, a aplicação iniciará a negociação de uma chave Diffie-Hellman(DH)[39, 40] que será utilizada para proteger a informação sensível a trocar entre o cliente e o servidor. Verificamos necessidade de estabelecer uma camada adicional de proteção para a troca de informação sensível, através da negociação de

uma chave secreta para o pedido, de forma a proteger por exemplo um PIN, impedindo que um utilizador com o auxílio de um *proxy* de análise de tráfego HTTP, com funcionalidades de Men in the Middle, realizar a interceção do PIN. Um exemplo deste tipo de *proxies* é o WebScarab[41] que poderia ser empregue para efetuar este tipo de ataque. A chave, partilhada entre as partes, pretende ser mais uma ferramenta de segurança da aplicação contra ataques realizados pelo cliente à informação trocada entre as aplicações, dado permitir proteger a aplicação de ataques realizados através de um *proxy* à comunicação TLS.

Utilizando a chave calculada, a aplicação servidor, após a autenticação do utilizador e realizada a validação das suas permissões, devolverá um documento XML contendo várias informações do utilizador que a aplicação cliente necessitará para continuar com a personalização do Cartão U.PORTO. Com a informação recebida, e se a autenticação tiver sido bem-sucedida, inicia-se um conjunto de processos de verificação do cartão universitário. Em caso negativo a aplicação cliente termina.

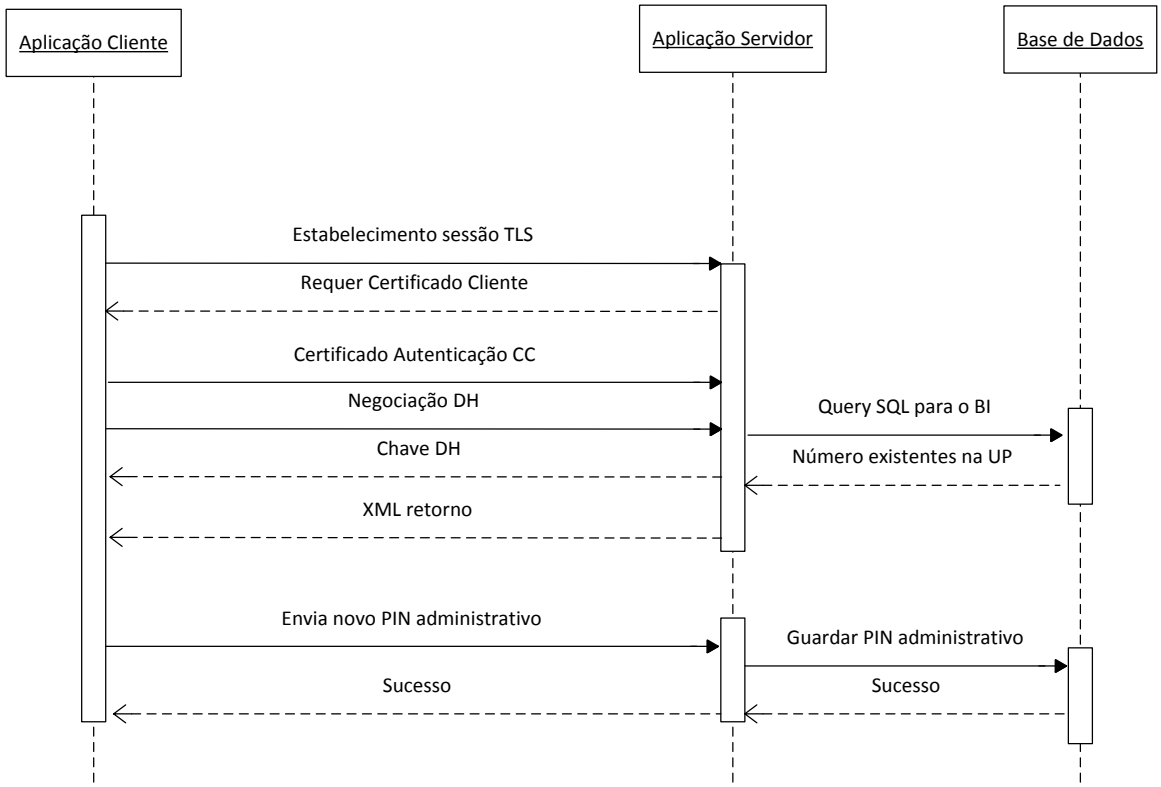


Ilustração 5 - Esquema de comunicações da fase inicial

Tal como se pode verificar na ilustração 5 (Esquema de comunicações de fase inicial), a primeira verificação realizada, é a identificação do cartão presente no leitor. Pretende-se com este procedimento detetar se está introduzido um *smart card* válido antes sequer de realizar qualquer outra ação. A verificação é realizada através da comparação do valor do *Answer To Reset* (ATR) com o identificado para o Cartão U.PORTO em circulação. O ATR é a mensagem devolvida pelo cartão conforme a ISO/IEC 7816, após o *reset* da energia elétrica enviada pelo leitor ao cartão. O ATR fornece informações sobre os parâmetros de comunicação necessários para utilizar o cartão e para obter informações sobre o seu modelo e estado. Com a validação do Cartão U.PORTO e a garantia de que está perante um cartão com um ATR conhecido, a aplicação inicia a validação do titular do cartão, enviando uma sequência de comandos *Aplication Protocol Data Units* (APDU) que lhe permitem inicializar a aplicação personalizada

pela SIBS Cartões no momento de produção do cartão e obter a informação sobre a identidade do titular enviada pela Universidade. Esta aplicação retorna a informação gravada no chip, que após a sua personalização se encontra no estado *read only* e que, por seu turno, permite obter informação importante para a implementação do nosso projeto: N.º de Estudante/Colaborador; Categoria; Ano de Frequência; Ano Letivo ou Civil; Faculdade, Instituto ou Departamento; Cartão Ativo ou Inativo; Data de Validade; N.º de cartão não bancário.

Com a obtenção da informação armazenada no chip do cartão, a aplicação cliente poderá verificar na informação devolvida pelo servidor se o cliente é o titular do cartão. Em caso afirmativo a aplicação segue para o próximo passo, caso contrário, a aplicação informa o servidor da falha detetada na sessão e termina.

Após realizada a validação do titular do Cartão U.PORTO inicia-se o processo de personalização do código pessoal PIN, que, por regras impostas pelo fabricante Gemalto, deverá ter um comprimento igual a seis. No momento de definição do código pessoal é também alterado o código PIN administrativo, de forma a garantir que o cartão fica personalizado para o seu titular e o nível de administração fica assim também protegido de possíveis ataques. Este PIN administrativo é único para cada cartão, gerado pela aplicação servidor através de uma operação aritmética, calculando o valor do código através do número de série do cartão e uma chave privada conhecida unicamente pelo servidor.

Com a personalização do código pessoal, consideramos o cartão pronto para ser utilizado em ambientes criptográficos, ficando disponível a opção para geração do par de chaves (privada e pública) e solicitação do certificado X.509[42]. Nesse momento poderá ainda ser importado um certificado com o respetivo par de chaves através de um objeto PKCS#12[43]. A segunda hipótese será utilizada nos certificados com a finalidade de cifrar informação.

A geração do par de chaves é concretizada através da interface PKCS#11 do *middleware* do Cartão U.PORTO. O PKCS#11 pertence à família dos *standards* Public-Key Cryptography Standards (PKCS), publicado pelos laboratórios RSA, e define uma API independente da plataforma para *tokens* criptográficos, como é o caso dos *smart cards*. No âmbito deste projeto de trabalho, será utilizada a implementação existente no Java *Cryptography Architecture* (JCA)[44] e o Java *Cryptography Extension* (JCE). Esta interface permite inicializar o dispositivo criptográfico, garantindo privilégios de escrita e geração de chaves no chip do *smart card*. Após

a geração do par de chaves é produzido um *certificate signing request* (CSR) a enviar à Entidade Certificadora (EC) para assinatura. No âmbito deste projeto a operação de envio à EC é realizada através da aplicação Confusa. A integração das aplicações será analisada no ponto seguinte desta dissertação.

A implementação da solução para os certificados de cifra, passa pela importação do objeto PKCS#12. O criptocontentor gerado pela PKI contendo o certificado e respetivo par de chaves, foi implementada utilizando a aplicação servidor como cliente da aplicação EJBCA. Para o efeito, e aproveitando o facto de o EJBCA disponibilizar uma interface de *webservices*, a aplicação servidor invoca o respetivo serviço e recolhe o objeto PKCS#12 contendo a chave de cifra do utilizador. Este objeto é depois devolvido pelo servidor à aplicação cliente que o importa para o Cartão U.PORTO, para a *slot* respetiva utilizando a interface PKCS#11. No final deste processo o cartão encontra-se inicializado, com o PIN do utilizador definido e o pedido de certificado realizado. O titular terá unicamente que aguardar que a EC devolva o seu certificado assinado. A aplicação Confusa, utilizada para gerir a submissão do pedido do certificado à EC Comodo, gere o estado da assinatura, notificando o utilizador quando o pedido se encontra disponível para recolha, via correio eletrónico ou diretamente no portal. Após receber a informação de disponibilidade, o utilizador tem acesso a uma nova aplicação cliente, com uma interface mais simples, bastando-lhe indicar o PIN definido e solicitar a importação do certificado para concluir o processo de personalização do Cartão U.PORTO. Aproveitamos esta fase para informar a aplicação servidor de que o certificado foi gerado, adicionando-o à base de dados e disponibilizando-o aos serviços de LDAP e AD.

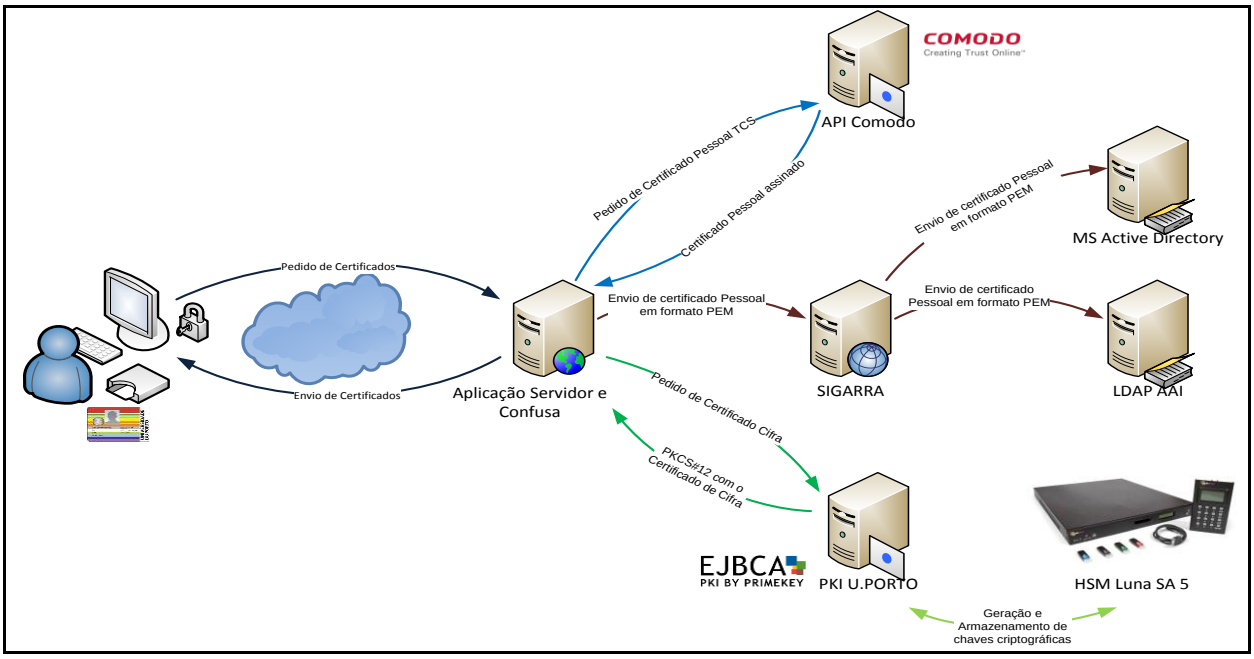


Ilustração 6 - Arquitetura global proposta

Com a conclusão do processo de personalização do Cartão U.PORTO este fica pronto a ser utilizado pelo seu titular, conforme ilustra a seguinte imagem (Ilustração 7).

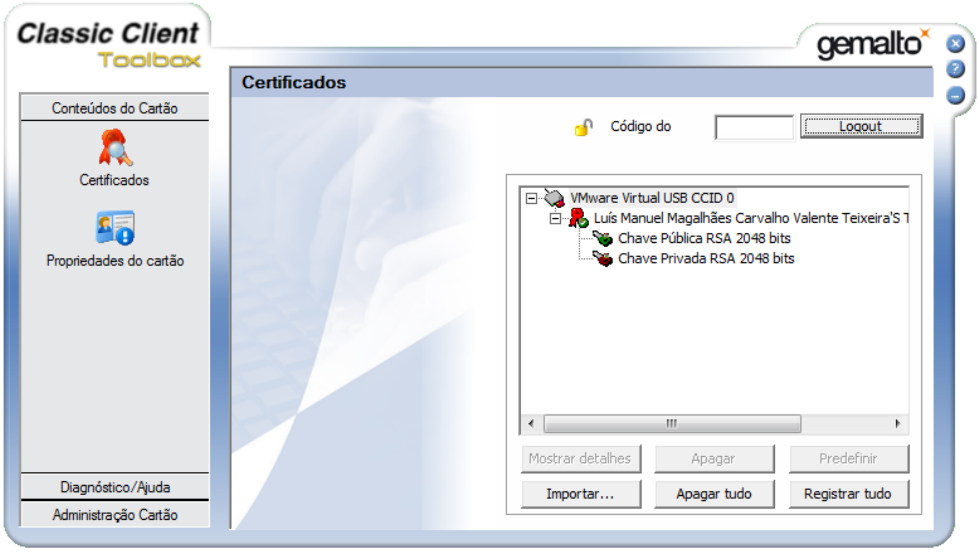


Ilustração 7 - Cartão U.PORTO personalizado

O Cartão U.PORTO poderá então ser utilizado nos vários serviços e aplicações, assinatura digital de documentos e correio eletrónico, autenticação *online* e em postos de trabalho, bem como na cifra de informação, tal como exemplifica a ilustração 8 - Utilizações possíveis com o Cartão U.PORTO.

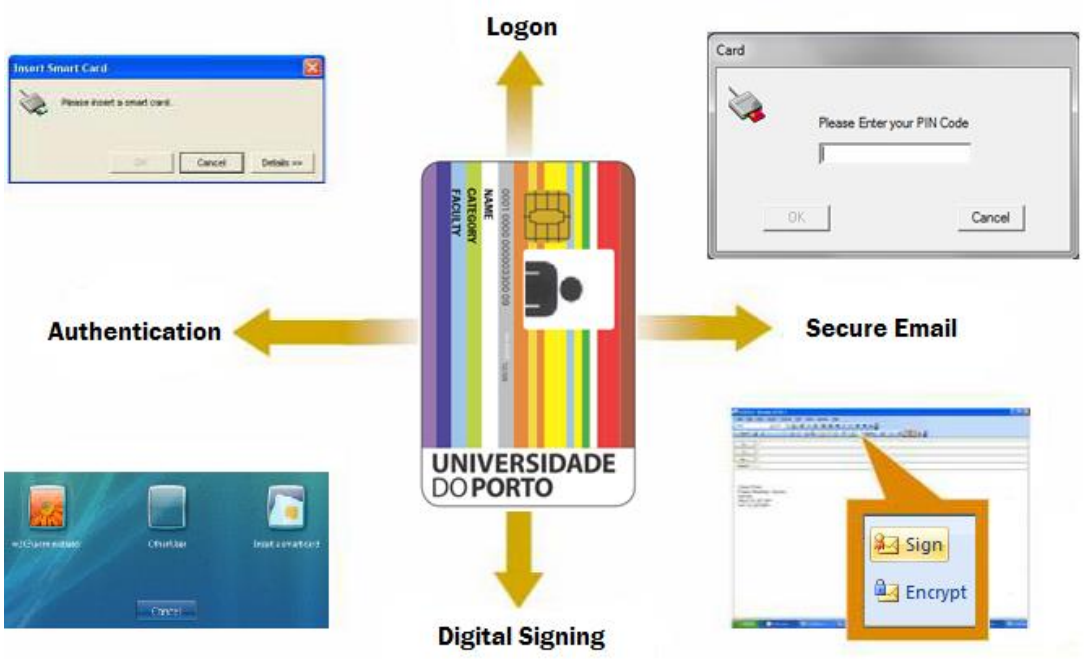


Ilustração 8 - Utilizações possíveis com o Cartão U.PORTO

4.2. Integração – Cartão U.PORTO e Confusa

A opção tomada pela U.PORTO pela utilização dos certificados digitais emitidos pela EC COMODO, via serviço TCS da TERENA, obrigou-nos a utilizar a aplicação Confusa para acesso à API da COMODO, esta aplicação serve de interface aos utilizadores das IES para emissão de certificados digitais x.509. A utilização desta aplicação foi nos imposta pela entidade fornecedora do serviço (FCCN), surgindo assim a necessidade de integrarmos o nosso projeto com esta aplicação.

Confusa é uma aplicação *open-source* desenvolvida sobre uma *framework* PHP pela UNINETT e pela Nordic DataGrid Federation, destinada à gestão de certificados pessoais. A aplicação dispõe de uma interface gráfica de fácil customização utilizando autenticação federada via *Shibboleth[45]*, para recolher atributos dos utilizadores, validar os dados do pedido e verificar as permissões do utilizador antes da emissão dos certificados. A aplicação pode ser utilizada para a assinatura de certificados através da API da Comodo ou certificados *self-sign.*

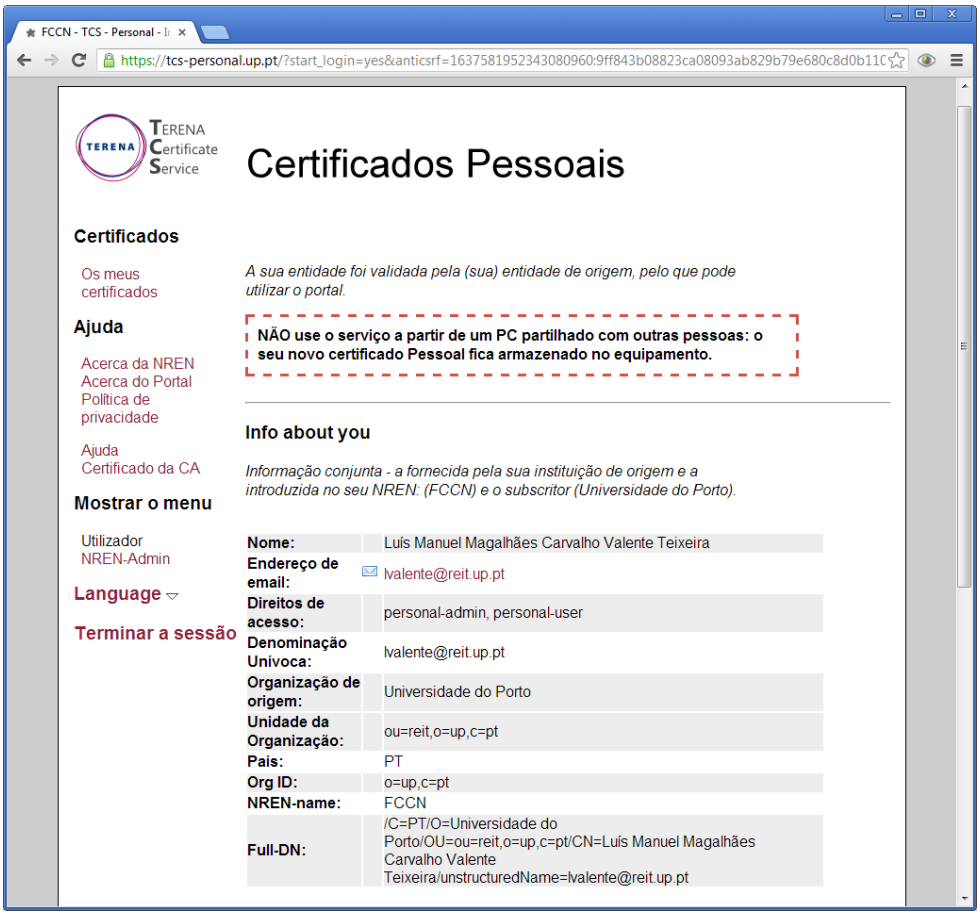


Ilustração 9- Interface - Confusa

A Confusa pode ser utilizada por múltiplas IES ou até partilhada por múltiplas NREN. A TERENA disponibiliza ainda a aplicação como um serviço, possibilitando às NREN a sua utilização mediante o pagamento de um custo anual de manutenção do mesmo. No caso português, a FCCN, conjuntamente com a U.PORTO, optou por implementar e disponibilizar este serviço a nível nacional, tendo a U.PORTO ficado responsável pela infraestrutura tecnológica e manutenção do serviço. Ao nível da solicitação de certificados digitais, a Confusa foi desenvolvida de forma a permitir três alternativas de pedido do certificado: a) gerando o certificado no *browser* cliente, utilizando os repositórios de certificados a que o navegador tem acesso; b) possibilitando que o utilizador cole o texto do Certificate Signing Request (CSR) no formulário; c) fazendo o *upload* do ficheiro que contém o pedido de certificado. O pedido é tratado pela aplicação, extraindo do CSR os atributos pessoais que o utilizador definiu e enviando a chave pública juntamente com os atributos recolhidos da autenticação *Shibboleth* para a API da Comodo. Normalmente a assinatura do pedido pela Entidade Certificadora Comodo ocorre em tempo real. Durante o processo, o utilizador é reencaminhado para um ecrã onde aguarda a resposta da EC. Se a resposta não puder ser dada imediatamente, o utilizador será notificado por correio eletrónico quando o seu certificado se encontrar disponível para ser descarregado.

O utilizador tem acesso aos certificados disponíveis através do separador “Os meus Certificados”, onde dispõe de opções para descarregar o certificado, importá-lo para a *keystore*, no caso do nosso projeto para o *smart card*, e revogar o certificado.

4.2.1. Pedido de Certificado

A aplicação cliente desenvolvida no âmbito deste projeto, foi integrada com o código da Confusa que já permitia a submissão de pedidos de certificados através do preenchimento de um formulário com o CSR (ilustração 10). Assim, após realizados todos os procedimentos necessários pela aplicação cliente, e garantida a geração do par de chaves, é criado o respetivo CSR, que é enviado pelo Confusa à API da COMODO. A imagem seguinte ilustra como enviar ou criar um CSR.

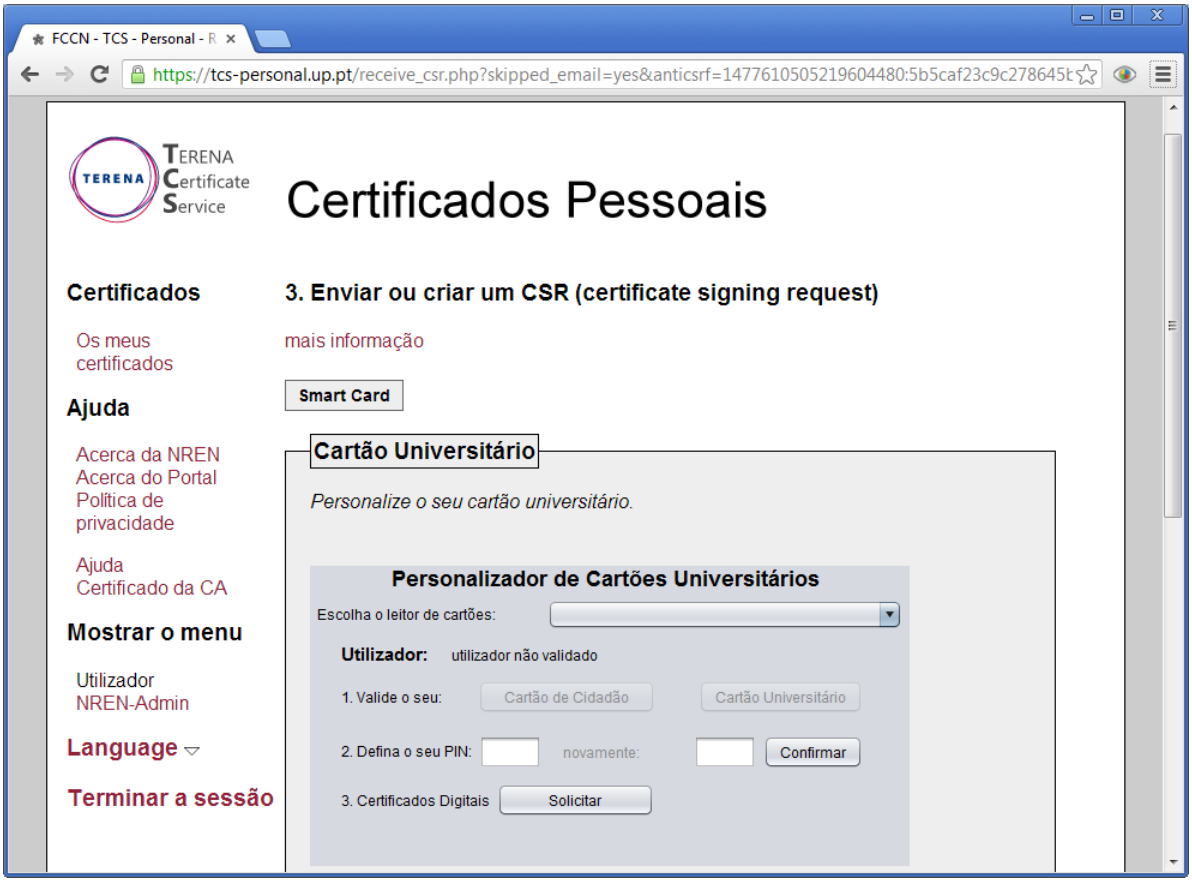


Ilustração 10 – Interface de pedido de certificados

Para permitir esta integração foi desenvolvida uma pequena função em *Javascript (ilustração 11)* que é invocada pela aplicação cliente, enviando como argumento o CSR. Esta função é responsável por preencher o campo csrBox já existente na implementação original do Confusa, tal como ilustra a imagem seguinte.

```
4   function setCsrBox(pkcs10Csr) {
5       var obj2=document.getElementById('csrBox');
6       obj2.value+=pkcs10Csr;
7       $('#nextButton').attr("disabled", false);
8   }
```

Ilustração 11- Função para preenchimento da csrBox

4.2.2. Importação do Certificado

Após a assinatura do certificado pela EC Comodo, a aplicação Confusa permite ao utilizador a importação do mesmo para o *smart card*. Para tal foi desenvolvida uma *applet* específica para esta função (ilustração 12). A *applet* obtém do Confusa o certificado a importar para o cartão e solicita ao utilizador o código PIN que definiu anteriormente de forma a concluir a importação do certificado.

Ilustração 12 – Importação do certificado digital para o Cartão U.PORTO

No caso da importação do certificado, a aplicação é inicializada com um parâmetro que lhe permite conhecer qual é o certificado que o utilizador está a solicitar e desta forma invocar uma função *Javascript* que lhe retorna o certificado em formato PEM (ilustração 13).

```
5  function getCert(num) {
6      var obj=document.getElementById("cert"+num);
7      personalize.input = obj.innerHTML;
8  }
```

Ilustração 13 - Função para recolha do certificado em formato PEM

4.3. Aplicação Cliente

A aplicação cliente é responsável por validar o cartão universitário do utilizador e estabelecer uma sessão segura TLS com a aplicação servidor, utilizando para o efeito o certificado de autenticação presente no Cartão de Cidadão.

Ao nível de interface gráfico pretendeu-se criar um interface simples, de fácil utilização e intuitivo, como demonstra a ilustração 14 - Interface gráfico para a personalização. As opções para o utilizador são ativadas conforme este vai avançando no processo de personalização do Cartão U.PORTO.

A aplicação cliente foi desenvolvida sobre tecnologia JAVA, sendo assim compatível com vários sistemas operativos e sob a forma de uma JApplet, permitindo a sua utilização em ambiente *web*. Procurámos ainda utilizar, sempre que possível, as bibliotecas existentes na Java Virtual Machine (JVM), sendo unicamente dependente das bibliotecas dos *middleware* dos *smart cards* utilizados, Cartão de Cidadão e Cartão U.PORTO.

Ilustração 14 - Interface gráfico para a personalização

A aplicação cliente é composta por um conjunto de classes que formam esta aplicação, o interface gráfico é gerado pela classe Cliente.class estendendo a classe javax.swing.JApplet. Nesta também se encontram implementados os métodos necessários para execução da *applet* e implementada a arquitetura estabelecida.

No momento de inicialização da aplicação são gerados os elementos gráficos, a classe que contém a informação sobre o utilizador e informações estáticas, sendo ainda inicializadas as configurações do ambiente de execução da aplicação.

Num primeiro momento, utilizando a biblioteca Java SmartCardIO (Ilustração 15 - Inicialização SmartCardIO), em que se realiza um inventário dos leitores de cartões existentes na máquina cliente e com esses dados recolhidos, personaliza-se a *combobox* que permite ao utilizador a seleção no interface da aplicação do leitor onde se encontra o *smart card* que irá utilizar.

```
128     private void initSettings() {
129
130         File tmp = info.getLibPcscLite();
131         if (tmp.exists()) {
132             System.setProperty("sun.security.smartcardio.library", tmp.getAbsolutePath());
133         }
134
135         try {
136             //Adquire Fabrica de Leitores
137             factory = TerminalFactory.getDefault();
138             System.out.println("Provider : " + factory.getProvider());
139
140             //Adquire Lista de Leitores PC/SC no Sistema
141             terminals = factory.terminals().list();
142             System.out.println("Lista : " + terminals);
143
144             //Adiciona termiais a ComboBox
145             terminalBox.removeAllItems();
146             for (Object s : terminals.toArray()) {
147                 terminalBox.addItem(s);
148             }
149
150
151         } catch (Exception e) {
152             e.printStackTrace(System.out);
153             JOptionPane.showMessageDialog(frame, e.getMessage());
154                 stop();
155         }
156     }
```

Ilustração 15 - Inicialização SmartCardIO

4.3.1. Autenticação com o Cartão de Cidadão

Após a inicialização da applet torna-se disponível ao utilizador a opção para se autenticar, utilizando para o efeito o seu Cartão de Cidadão. A ação despoletada pelo clicar no botão inicializa a biblioteca libpteidpkcs11 que permite à JVM comunicar com o interface PKCS#11 do Cartão de Cidadão e, desta forma aceder à keystore que contém o Certificado de Autenticação. Na ilustração 16, podemos verificar a inicialização da truststore para Autenticação com CC.

A comunicação entre a aplicação cliente e servidor realiza-se sobre uma comunicação protegida por TLS com obrigatoriedade de autenticação do cliente através de um certificado X.509 cliente válido. Por sua vez, a aplicação cliente também só aceita estabelecer comunicações com servidores para os quais conhece e confia na sua hierarquia de certificação do certificado apresentado. Verificando-se que poderá ser difícil garantir que todas as JVM clientes dispõem da cadeia de certificação completa dos servidores, é fornecido juntamente com a aplicação cliente o conjunto de certificados a utilizar, que por sua vez irão dar lugar a uma *truststore* gerada pela execução do código da aplicação e que em nada interfere com as já existentes na máquina cliente.

```
468     private void initCC() {
469         try {
470             CertificateFactory certificateFactory = CertificateFactory.getInstance("X509");
471
472             String[] certs = {"MIIENjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUIxJjAk
473             KeyStore truststore = KeyStore.getInstance(KeyStore.getDefaultType());
474             truststore.load(null, null);
475
476             for (String cert : certs) {
477                 byte[] publicKeyBytes;
478                 publicKeyBytes = javax.xml.bind.DatatypeConverter.parseBase64Binary(cert);
479                 Certificate certificate = certificateFactory.generateCertificate(new ByteArrayInputStream(publicKeyBytes));
480                 //System.out.println("Certificado: " + certificate.getPublicKey());
481                 X509Certificate x509 = (X509Certificate) certificate;
482                 //System.out.println("Certificado2: " + x509.getSubjectDN().getName().substring(3, 15).replace(" ",""));
483                 truststore.setCertificateEntry(x509.getSubjectDN().getName().substring(3, 15).replace(" ", ""), certificate);
484
485             }
```

Ilustração 16 -Inicialização da *truststore* para Autenticação com CC

Seguidamente é adicionada a *keystore* que contém os certificados a utilizar para a autenticação do cliente. Neste caso concreto, é utilizada a interface PKCS#11 para permitir de forma transparente, a conexão ao *smart card*, tal como representa a ilustração 17 - Inicialização da keystore PKCS#11 do CC.

```
487             byte[] pkcs11configBytes = info.getPkcs11ConfigSettings().getBytes();
488             ByteArrayInputStream configStream = new ByteArrayInputStream(pkcs11configBytes);
489             Provider pkcs11Provider = new sun.security.pkcs11.SunPKCS11(configStream);
490             Security.addProvider(pkcs11Provider);
491
492             try {
493
494                 //Load KeyStore
495                 KeyStore smartCardKeyStore = KeyStore.getInstance("PKCS11");
496                 smartCardKeyStore.load(null, null);
```

Ilustração 17 - Inicialização da keystore PKCS#11 do CC

Antes de realizar a conexão para o servidor, existe a necessidade de configurar o contexto da sessão, para tal é definido a *truststore* e *keystore* da conexão. Na ilustração seguinte, podemos ver como se procede o estabelecimento de uma sessão TLS com autenticação através de certificado cliente.

```
507             KeyManagerFactory kmf = KeyManagerFactory.getInstance("SunX509");
508             kmf.init(smartCardKeyStore, null);
509
510             TrustManagerFactory tmf = TrustManagerFactory.getInstance(TrustManagerFactory.getDefaultAlgorithm());
511             tmf.init(truststore);
512
513             SSLContext sslCtx = SSLContext.getInstance("TLSv1");
514
515             KeyManagerFactory keyManagerFactory = KeyManagerFactory.getInstance("SunX509");
516             keyManagerFactory.init(smartCardKeyStore, null);
517
518             MyX509KeyManager customKeyManager = new MyX509KeyManager((X509KeyManager) keyManagerFactory.getKeyManagers()[0]);
519
520             sslCtx.init(new KeyManager[]{customKeyManager}, tmf.getTrustManagers(), null);
521             SSLSocketFactory sslfactory = sslCtx.getSocketFactory();
522
523             String data = URLEncoder.encode("client", "UTF-8") + "=" + URLEncoder.encode(clientDH, "UTF-8");
524
525             SSLSocket socket = (SSLSocket) sslfactory.createSocket("mobilitydev.up.pt", 443);
526
527             socket.setUseClientMode(true);
528             socket.startHandshake();
```

Ilustração 18 - Estabelecimento de uma sessão TLS com autenticação através de certificado cliente.

Seguidamente é criado um *socket* SSL para o servidor e iniciado o *handshake* com o servidor, garantindo a utilização de certificado de cliente.

Como resposta, a classe recebe um documento XML que é processado. Este documento se a autenticação tiver sido concluída com sucesso, contém os dados sobre o utilizador que permitirão validar o Cartão U.PORTO. Caso a autenticação falhe, o documento indica à aplicação cliente o erro e a aplicação encerra a sua execução.

Se a autenticação do utilizador tiver sido positiva passará a estar disponível no interface, a opção para validação do Cartão Universitário.

4.3.2. Validação Cartão Universitário

A validação do cartão universitário realiza-se por chamada da ação despoletada pelo clique do botão *tuiButton* que evoca o método validateTUI(). Este método começa por verificar qual o cartão que está presente no leitor e analisa se o mesmo pertence ao conjunto de cartões para os quais a aplicação está preparada, isto é, verifica se o ATR do cartão é coincidente com o valor definido na classe UserInfo.java. De seguida, analisa os dados de personalização do cartão, utilizando para o efeito o envio de comandos APDU que retornam as informações que foram gravados no cartão, no momento da sua personalização na SIBS Cartões. A ilustração 19 representa um exemplo de validação do cartão universitário.

```
587     private boolean valUserTUI() {
588         try {
589             // Aceder aos dados do TUI
590             //Adquire Canal de Comunicação
591             cardChannel = card.getBasicChannel();
592 
593             buffer = DatatypeConverter.parseHexBinary("00A4040008501649FF081492FF");
594 
595             //Monta APDU de Envio
596             commandAPDU = new CommandAPDU(buffer);    //AID
597 
598             responseAPDU = cardChannel.transmit(commandAPDU);
599             //Verifica Resposta
600             if (responseAPDU.getSW() != 0x9000) {
601 
602                 try {
603                     throw new Exception("Falha ao Selecionar : "
604                             + String.format("0x%04X",
605                             responseAPDU.getSW()));
606 
607                 } catch (Exception ex) {
608                     Logger.getLogger(Client.class.getName()).log(Level.SEVERE, null, ex);
609                     JOptionPane.showMessageDialog(frame, ex.getMessage());
610                 stop();
611                 }
612             }
```

Ilustração 19 - Validação do Cartão Universitário

4.3.3. Inicializar códigos PIN

O cartão universitário é produzido sem a personalização do código PIN para o utilizador. É portanto, na fase posterior à autenticação do utilizador à verificação do titular do Cartão U.PORTO, que este pode escolher um código PIN para o seu cartão. Este código deverá ter um tamanho igual a 6 dígitos, por definição da política utilizada pelo produtor do cartão.

Para a inicialização do código PIN é necessário um conjunto de códigos APDU que são enviados ao cartão, estes códigos estão definidos num *array*. A ilustração 20 mostra a forma de captura de comandos APDU. O conjunto de comandos APDU, necessários para a inicialização do Cartão U.PORTO, foi obtido através da análise da comunicação realizada entre aplicação Classic Cliente da Gemalto e o cartão. Esta informação foi obtida através de *logs* da implementação Personal Computer/Smart Card (PC/SC) Lite, que ao ser executada com determinados parâmetros e privilégios administrativos, permite visualizar toda a troca de informação entre as aplicações e os *smart cards*.

```
$ sudo pcscd --foreground --apdu --color
```

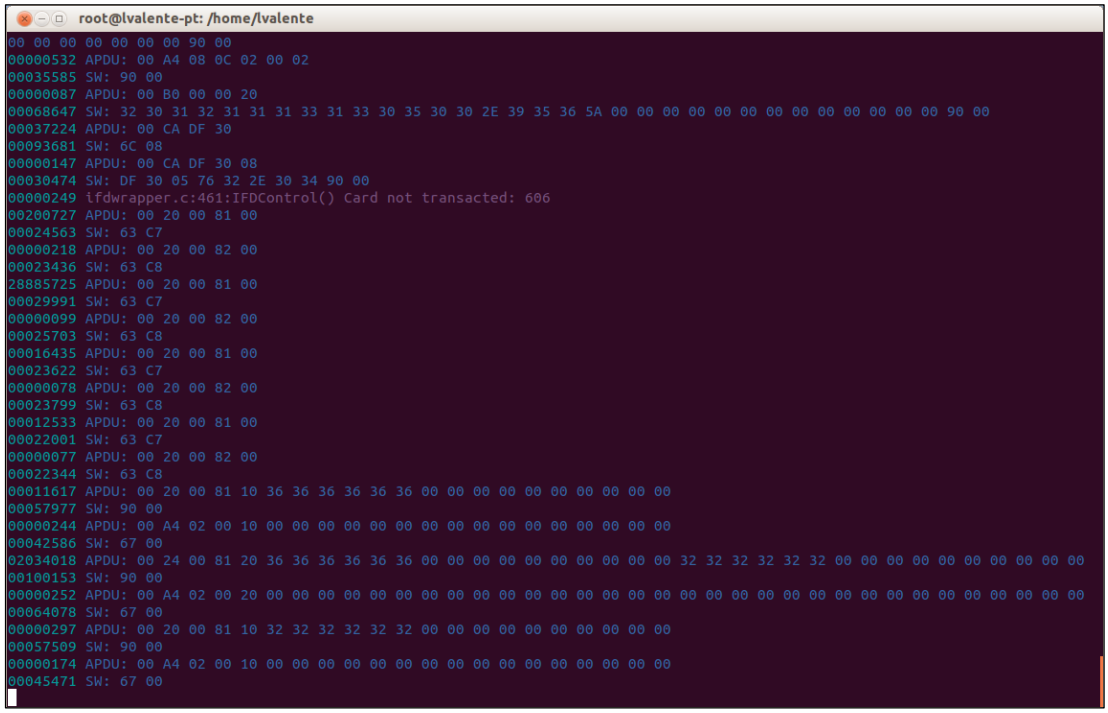


Ilustração 20 - Captura de comandos APDU

Antes de inicializar o cartão e para ter certeza que o utilizador sabe qual o PIN que está a definir, o código PIN é validado pelo método validateUserPin(), comparando os dois valores que foram solicitados aos utilizadores no interface.

Na ilustração 21, é possível verificar como é processada a criação do código PIN no Cartão U.PORTO.

```
732     private boolean initUserPin() {
733         String response = "";
734         if (validateUserPin()) {
735             try {
736 
737                 char[] tmpPinSO = info.getPinso();
738 
739                 System.out.println("tmpPinSO <= " + genAPDUdata(tmpPinSO));
740 
741                 //Adquire Canal de Comunicação
742                 cardChannel = card.getBasicChannel();
743                 String[] apdus = new String[]{"00A404000CA0000000180C000001634200",
744                     "00CA9F7F2D",
745                     "00A4080C020002",
746                     "00B0000020",
747                     "00CADF3008",
748                     "0020008100",
749                     "0020008200",
750                     "0020008110" + genAPDUdata(tmpPinSO) + "00000000000000000000",
751                     "0024008120" + genAPDUdata(tmpPinSO) + "00000000000000000000" + genAPDUdata(userPIN) + "00000000000000000000",
752                     "0020008110" + genAPDUdata(userPIN) + "00000000000000000000"
753                 };
754 
755                 for (String item : apdus) {
756                     buffer = DatatypeConverter.parseHexBinary(item);
757                     //Monta APDU de Envio
758                     commandAPDU = new CommandAPDU(buffer);      //AID
759 
760                     //Trasnmite e Recebe
761                     responseAPDU = cardChannel.transmit(commandAPDU);
762 
763                     response = formatBuffer(responseAPDU.getBytes(), responseAPDU.getBytes().length);
764                 }
765 
766             } catch (CardException ex) {
767                 Logger.getLogger(Client.class.getName()).log(Level.SEVERE, null, ex);
768                 JOptionPane.showMessageDialog(frame, ex.getMessage());
769                 stop();
770             }
771         } else {
772             JOptionPane.showMessageDialog(frame, "Falha ao validar PINs");
773         }
```

Ilustração 21 - Inicialização código PIN no Cartão U.PORTO

4.3.4. Geração de chaves e pedido de Certificado

Com a personalização de um PIN pessoal, o titular do cartão pode gerar um par de chaves pública e privada e, com este, é gerado o pedido de certificado CSR. A ilustração 22 mostra a geração do par de chaves no Cartão U.PORTO e respetivo CSR. A aplicação de destino do pedido, o Confusa, ignora os atributos constituintes do pedido de certificado X.509 contidos no CSR, substituindo pelos atributos respetivos recebidos da autenticação federada realizada pelo utilizador no acesso à aplicação, do pedido CSR utiliza a chave pública recebida para enviar à API da Comodo, o pedido de assinatura do certificado.

```
821     private void genKeys() {
822         try {
823             // TODO code application logic here
824             String pkcs11ConfigSettings = "name = SmartCardUP1\n" + "library = /usr/lib/pkcs11/libgclib.so\n" + "slot=" +
825 ->->->(slot + 1) + "\n" + "attributes(generate,*,*) = { CKA_TOKEN = true } \n attributes(generate,CKO_PUBLIC_KEY,*) = {
            CKA_ENCRYPT = false CKA_VERIFY = true CKA_WRAP = true } \n attributes(generate, CKO_PRIVATE_KEY,*) = {
            CKA_EXTRACTABLE = false CKA_DECRYPT = false CKA_SIGN = true CKA_UNWRAP = true }";
826
827             byte[] pkcs11configBytes = pkcs11ConfigSettings.getBytes();
828             ByteArrayInputStream configStream = new ByteArrayInputStream(pkcs11configBytes);
829
830             //Adiciona proverdor critografico do CUP
831             Provider p = new sun.security.pkcs11.SunPKCS11(configStream);
832             Security.addProvider(p);
833
834             KeyStore keystore = KeyStore.getInstance("PKCS11");
835             keystore.load(null, userPIN);
836
837             //Generate a PKCS11 keypair
838             KeyPairGenerator keyGenerator = KeyPairGenerator.getInstance("RSA", p);
839             System.out.println(keyGenerator.getProvider().getInfo());
840             keyGenerator.initialize(2048);
841             KeyPair keypair = keyGenerator.genKeyPair();
842             PrivateKey privateKey = keypair.getPrivate();
843             PublicKey publicKey = keypair.getPublic();
844
845             String sigAlg = "MD5WithRSA";
846             PKCS10 pkcs10 = new PKCS10(publicKey);
847             Signature signature = Signature.getInstance(sigAlg);
848             signature.initSign(privateKey);
849
850             X500Name x500Name = new X500Name("Nome do Utilizador", "Unidade Organica", "UPORTO", "PT");
851             pkcs10.encodeAndSign(x500Name, signature);
852
853             ByteArrayOutputStream bs = new ByteArrayOutputStream();
854             PrintStream ps = new PrintStream(bs);
855             pkcs10.print(System.out);
856             pkcs10.print(ps);
857
```

Ilustração 22 - Geração do par de chaves no Cartão U.PORTO e respetivo CSR

4.4. Aplicação Servidor

A aplicação no servidor é suportada pelo servidor aplicacional Tomcat na versão 7, com as devidas configurações para solicitar autenticação com certificado cliente no acesso à aplicação. Foram ainda adicionadas as condições necessárias à validação do certificado de autenticação do Cartão de Cidadão com a indicação de uma *truststore*. Desenvolvemos ainda uma extensão ao módulo de autenticação do Tomcat de forma a retornar às aplicações o atributo SERIALNUMBER do *distinguished name* (DN) do certificado do CC, o que corresponde ao número do BI.

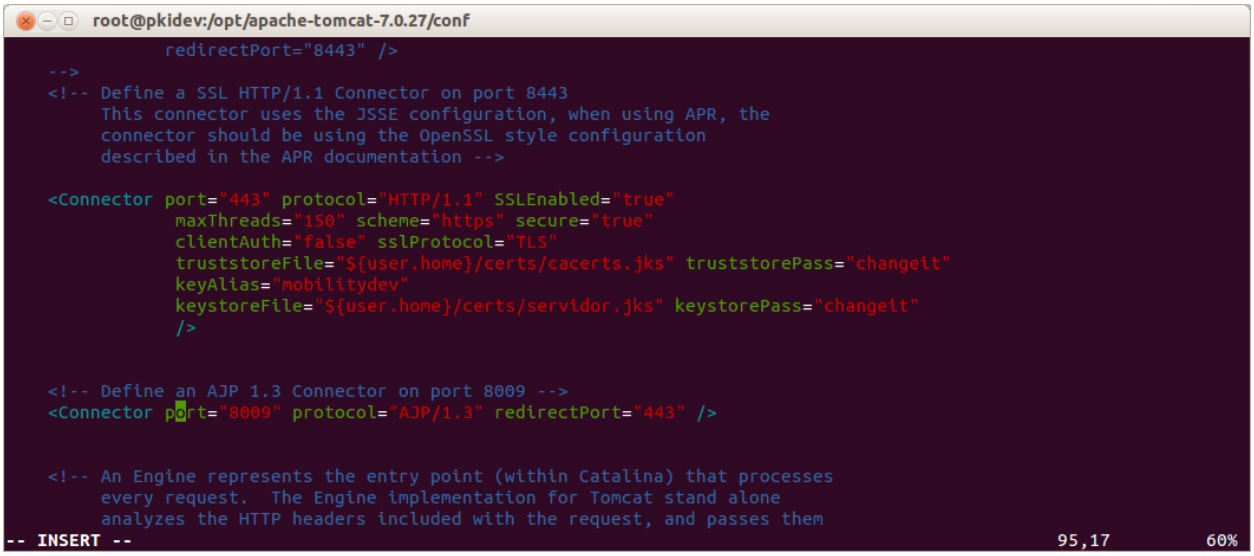


Ilustração 23 - Configuração do server.xml

```
root@pkidev:/opt/apache-tomcat-7.0.27/conf

      <!-- This Realm uses the UserDatabase configured in the global JNDI
           resources under the key "UserDatabase".  Any edits
           that are performed against this UserDatabase are immediately
           available for use by the Realm.  -->

      <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
             X509UsernameRetrieverClassName="X509SubjetcDnGetBI"  resourceName="UserDatabase"
      />
      </Realm>

     <Host name="localhost"  appBase="webapps"
           unpackWARs="true" autoDeploy="true">

      <!-- SingleSignOn valve, share authentication between web applications
           Documentation at: /docs/config/valve.html -->
      <!--
      <Valve className="org.apache.catalina.authenticator.SingleSignOn" />
      -->

      <!-- Access log processes all example.
           Documentation at: /docs/config/valve.html
           Note: The pattern used is equivalent to using pattern="common" -->
-- INSERT --                                                    132,1         93%
```

Ilustração 24 - Configuração do *Realm* para autenticação com o CC

```
root@pkidev:/opt/apache-tomcat-7.0.27/webapps/Thesis-server/WEB-INF
        </session-timeout>
    </session-config>
    <security-constraint>
        <display-name>SecurityConstraint1</display-name>
        <web-resource-collection>
            <web-resource-name>WRCollection</web-resource-name>
            <description/>
            <url-pattern>/*</url-pattern>
        </web-resource-collection>
        <auth-constraint>
            <description/>
            <role-name>loginUser</role-name>
        </auth-constraint>
    </security-constraint>
    <login-config>
        <auth-method>CLIENT-CERT</auth-method>
    </login-config>
    <security-role>
        <description/>
        <role-name>loginUser</role-name>
    </security-role>

    <resource-ref>
                                                                 36,1          65%
```

Ilustração 25 - Configuração do web.xml da aplicação para requerer Certificado cliente

Além das *servlets* específicas para o funcionamento da solução, é reaproveitado o facto das configurações de autenticação serem geridas no contexto da aplicação web e aproveitando o motor de autenticação do servidor aplicacional.

```
root@pkidev:/opt/apache-tomcat-7.0.27/logs
192.168.212.26 - BI12847065 [19/Sep/2012:00:06:50 +0100] "GET /Thesis-server/validateuser?client=MIIBpjCCARsGCSqGSIb3
DQEDATCCAQwCgYEAxMNMOr8aYobcHQg0zlqRI%2FfwkqKKOGrMAlRubcruA2fYdMIfJYcuFO0YNZZMKG7SQXMGmfGBROIy98R4TMMkHg9IbslCueT8Xor
UNaSetLSYjH3RLuY5cxo7ciz4X50SlGYQBDtTtqqFIh8u3oMfv4vk2uogXo94RGIZzF07WvsCgYEAovcQXL3LeJi995EpskrTc0A4dgKejsQadn%2BmG4
%2BQ8UP9bgHImSUlZ1X%2BrieZ6nLbl4yCREEpcLP7pB5NKi8cIqM8KebAadbLQSWYgsI4g%2BwC7WwXu65IIFKDW099XbmkAEDLmAZswlyPDB2q3Ut8b
kveL45kpdaZUV99gKj6nJ4CAgP%2FA4GEAAKBgGe7hg8SU5%2FWsaSggDEOTY0aUGdThm2i4lfbbUlDyPkV9kVt1zdXWSD0qT3JUHj1pVWGH8Phs4jL43
%2FDj2r7V2y6xjLiJ8PbLhVaP0vVxLSY2vCiiRCo7djnu%2FBX7nyUqBBP%2F6h3ZPhuVa6vJN%2FnNU4iTY5wRyozK4MXFLUA4yL5 HTTP/1.0" 200
990
192.168.212.26 - BI12847065 [19/Sep/2012:00:09:08 +0100] "GET /Thesis-server/validateuser?client=MIIBpjCCARsGCSqGSIb3
DQEDATCCAQwCgYEAxMNMOr8aYobcHQg0zlqRI%2FfwkqKKOGrMAlRubcruA2fYdMIfJYcuFO0YNZZMKG7SQXMGmfGBROIy98R4TMMkHg9IbslCueT8Xor
UNaSetLSYjH3RLuY5cxo7ciz4X50SlGYQBDtTtqqFIh8u3oMfv4vk2uogXo94RGIZzF07WvsCgYEAovcQXL3LeJi995EpskrTc0A4dgKejsQadn%2BmG4
%2BQ8UP9bgHImSUlZ1X%2BrieZ6nLbl4yCREEpcLP7pB5NKi8cIqM8KebAadbLQSWYgsI4g%2BwC7WwXu65IIFKDW099XbmkAEDLmAZswlyPDB2q3Ut8b
kveL45kpdaZUV99gKj6nJ4CAgP%2FA4GEAAKBgCRWVS0urbcuz14bOAdVbX%2FSi2GftD2HScLUxSR8JcHp%2F7WRoa3uKTu7vKiLtwyn6NpnawpUwHSE
nXxLet4w%2FlP6tneDZUO7i2kn8iIa%2F%2BGJtS9ceA00JoSw8ZZJdrvtc4ODoCSfurM88OFCQPnSDYAXSCqXh2txljzYP7nd9NX8 HTTP/1.0" 200
994
192.168.212.26 - BI12847065 [19/Sep/2012:00:10:32 +0100] "GET /Thesis-server/validateuser?client=MIIBpjCCARsGCSqGSIb3
DQEDATCCAQwCgYEAxMNMOr8aYobcHQg0zlqRI%2FfwkqKKOGrMAlRubcruA2fYdMIfJYcuFO0YNZZMKG7SQXMGmfGBROIy98R4TMMkHg9IbslCueT8Xor
UNaSetLSYjH3RLuY5cxo7ciz4X50SlGYQBDtTtqqFIh8u3oMfv4vk2uogXo94RGIZzF07WvsCgYEAovcQXL3LeJi995EpskrTc0A4dgKejsQadn%2BmG4
%2BQ8UP9bgHImSUlZ1X%2BrieZ6nLbl4yCREEpcLP7pB5NKi8cIqM8KebAadbLQSWYgsI4g%2BwC7WwXu65IIFKDW099XbmkAEDLmAZswlyPDB2q3Ut8b
kveL45kpdaZUV99gKj6nJ4CAgP%2FA4GEAAKBgGW9aGil%2BnBEXSpsOwksEfDYYkXNHhWA8oESdOnNtryspXbNpPhl8I07viZ24ihOeKyrJ%2F%2FVCX
UmZImtbDWCbiSidk8xI8nzJUJ9ZZFEHCl4NG%2BcaebJ1BFKLVLOTs5SYRNCZOYfIMXubc12PNrtUm%2BL9eRjV890xXSV6UfZp4XR HTTP/1.0" 200
990
192.168.212.26 - BI12847065 [19/Sep/2012:00:19:00 +0100] "GET /Thesis-server/validateuser?client=MIIBpzCCARsGCSqGSIb3
DQEDATCCAQwCgYEAxMNMOr8aYobcHQg0zlqRI%2FfwkqKKOGrMAlRubcruA2fYdMIfJYcuFO0YNZZMKG7SQXMGmfGBROIy98R4TMMkHg9IbslCueT8Xor
:
```

Ilustração 26 - Output da autenticação com o CC no servidor TOMCAT

A servlet ValidateUser é responsável por validar o utilizador, verificar na base de dados a sua existência e a devolução da chave pública DH calculada. Neste momento é também calculada a chave privada DH com a qual é gerado um segredo, que permitirá cifrar a informação a enviar pelo servidor, à aplicação cliente.

```
98
99          response.setContentType("text/xml;charset=UTF-8");
100
101         XMLStreamWriter xsw = XMLOutputFactory.newInstance().createXMLStreamWriter(response.getWriter());
102         xsw.writeStartDocument("UTF-8", "1.0");
103         xsw.writeStartElement("userInfo");
104         xsw.writeAttribute("remote", request.getRemoteAddr());
105
106
107
108         if (cipherSuite != null) {
109             X509Certificate certChain[] = (X509Certificate[]) request.getAttribute("javax.servlet.request.X509Certificate");
110
111             //VALIDAR USER
112             if (certChain.length != 0) {
113                 String sujeito = certChain[0].getSubjectDN().toString();
114                 String dadosCert[] = sujeito.split(", ");
115                 for (String dado : dadosCert) {
116                     String temp[] = dado.split("=");
117                     if (temp[0].equals("SERIALNUMBER")) {
118                         userCivilNumber = temp[1].replace("BI", "");
119                         setlogs(st, "access", request.getRemoteAddr(), session.getId(), userCivilNumber);
120
121                     }
122                     xsw.writeStartElement(temp[0]);
123                     xsw.writeCharacters(temp[1]);
124                     xsw.writeEndElement();
125                 }
126             }
127
```

Ilustração 27- Produção da resposta XML

O certificado cliente é decomposto em várias componentes que por sua vez são processadas para o ficheiro XML (ilustração 27). Utilizando o certificado cliente recebido, verificamos quais os cartões existentes para o utilizador na base de dados e povoamos o XML com os dados obtidos (ilustração 28).

```
128             if (userCivilNumber != null) {
129                 rs = st.executeQuery("SELECT * FROM pessoa where idcivil=" + userCivilNumber);
130                 while (rs.next()) {
131                     userID = rs.getString("idpessoa")+";"+userID;
132
133                 }
134                 xsw.writeStartElement("idpessoa");
135                 xsw.writeCharacters(userID);
136                 xsw.writeEndElement();
137
138             }
```

Ilustração 28 - Recolha de dados sobre o utilizador da base dados

Pela aplicação é retornado um documento XML, contendo as informações necessárias à inicialização do cartão, se o processo de validação ocorrer sem erros. Em caso de erro, o documento é devolvido com um elemento de erro, com a informação pertinente para aplicação cliente.

Após a sessão ser validada, a aplicação regista na base de dados, o acesso realizado contribuindo assim para a facilitação de auditoria da aplicação, o utilizador que procedeu à autenticação, IP cliente, os segredos gerados e a sessão TLS do pedido. Por motivos ainda de segurança e auditoria, foi implementado o método setlogs(), que regista as ações a cada momento da aplicação, tal como se pode verificar na ilustração 29 - registo das operações na base de dados.

```
181     private void setlogs(Statement st, String param1, String param2, String param3, String param4) {
182         try {
183             String sql = "INSERT INTO logs (acao,ip,idsessao,DNserialnumder)VALUES('" + param1 + "','" + param2 + "','" + param3 +
                    "','" + param4 + "')";
184
185             int i = st.executeUpdate(sql);
186         } catch (SQLException ex) {
187             Logger.getLogger(ValidateUser.class.getName()).log(Level.SEVERE, null, ex);
188         }
189     }
190
191     private void setSession(Statement st, String param1, String param2, String param3, String param4, String param5) {
192         try {
193             String sql = "INSERT INTO sessao (idsessao,idpessoa,ipcliente,segredo,estado)VALUES('" + param1 + "','" + param2 +
                    "','" + param3 + "','" + param4 + "','" + param5 + "')";
194
195             int i = st.executeUpdate(sql);
196         } catch (SQLException ex) {
197             Logger.getLogger(ValidateUser.class.getName()).log(Level.SEVERE, null, ex);
198         }
199     }
```

Ilustração 29 - Registo das operações na base de dados

5. Conclusões e trabalho futuro

5.1. Resumo do trabalho de pesquisa

Fundamentalmente, atingimos o objetivo de desenvolver um protótipo de aplicação para a personalização criptográfica do Cartão U.PORTO, permitindo a geração e importação de certificados digitais X.509.

Numa primeira fase, apresentada no capítulo 2, realizámos um estudo sobre casos similares de utilização de cartões universitários procurando conhecer casos de utilização de *smart cards* com certificados digitais em IES e conhecer os respetivos processos de personalização. Do estudo dos vários exemplos verificámos ainda a necessidade de aprofundar o conhecimento da legislação sobre certificados digitais e o valor probatório da sua utilização no âmbito de operações de desmaterialização administrativa, vertido o trabalho no capítulo 3.

A investigação realizada foi vital para tomar conhecimento dos modelos de personalização de cartões implementados em IES e permitir a nossa escolha pelo modelo *self-service*, direcionando o nosso trabalho de pesquisa na procura das soluções e tecnologias que permitem implementar a solução escolhida. O protótipo foi desenvolvido implementando as ferramentas necessárias para permitir a personalização do Cartão U.PORTO e a sua integração com aplicações para a emissão e gestão de certificados, conforme demonstramos no capítulo 4.

5.2. Principais conclusões

A principal conclusão que este projeto permitiu alcançar, prende-se com o desenvolvimento de uma aplicação que permite a personalização criptográfica do Cartão U.PORTO de forma *self-service* e *user-centric.*

Associado à conclusão deste projeto, a Universidade passará a ter disponíveis ferramentas que lhe permitem implementar soluções de modernização administrativa, desmaterializando processos e paralelamente realizar um incremento da segurança e confiabilidade dos seus sistemas informáticos e informação.

5.3. Limitações da arquitetura proposta

A principal limitação da arquitetura proposta prende-se com a utilização das bibliotecas fornecidas pelo produtor do *middleware* do Cartão U.PORTO, isto é, a aplicação só poderá ser utilizada nos sistemas operativos suportados, que no caso do Classic Client são suportadas várias distribuições Linux, Microsoft Windows e algumas versões de MacOS.

Outra limitação inerente ao desenvolvimento da aplicação cliente encontra-se na necessidade do sistema operativo e *browser* cliente, de terem instalado a máquina virtual JAVA.

5.4. Trabalho futuro

No desenvolvimento de todo o protótipo foi planeado e identificada a forma de realizar a emissão de certificados para cifra e quais os mecanismos para o seu *backup*. De forma a aferir a admissibilidade desta solução, foram realizados testes com uma instalação em ambiente de desenvolvimento da aplicação EJBCA e a aplicação cliente com a finalidade de testar a emissão e importação de certificados digitais. Neste âmbito, ficou para trabalho futuro a implementação da aplicação EJBCA e a sua integração com o HSM numa arquitetura para utilização em ambiente de produção.

Toda a componente de integração com o SIGARRA dos certificados emitidos, particularmente com o módulo de Gestão de Identidades, que permite a propagação da informação sobre o utilizador para a infraestrutura de Autenticação e Autorização da U.PORTO, encontra-se ainda para desenvolvimento futuro.

5.5. Conclusão

A implementação desta dissertação foi um desafio bastante aliciante, uma vez que verificamos que não existem muitos exemplos de IES que utilizem *smart cards* com certificados digitais e não identificamos exemplos de implementações de soluções de personalização baseadas numa solução *user-centric* com elevados níveis de segurança e confiabilidade.

O desenvolvimento realizado procurou sempre a utilização de bibliotecas disponibilizadas em código aberto, mas deparamo-nos com certas dificuldades, pois algumas destas bibliotecas estão ainda a ser desenvolvidas e disponibilizadas, por exemplo, os mecanismos de autenticação com certificados digitais do Tomcat sofreram alterações no decorrer dos trabalhos. Acresce ainda às dificuldades sentidas, o fato de grande parte do trabalho estar a ser realizado sobre *middleware* e bibliotecas de código proprietário, com acesso à documentação limitado e restrito, o que no caso da Gemalto, demonstrou-se uma dificuldade acrescida e a cadência bastante demorada no aceso aos documentos, não contribuiu para o rápido desenrolar dos trabalhos. Se, no caso do Cartão de Cidadão existe bastante informação e manuais disponíveis na rede, relativamente ao Cartão U.PORTO o suporte e informação disponível pela Gemalto são limitados e verificaram-se insuficientes.

Mesmo perante estas dificuldades, foi possível através de bastante pesquisa e trabalho prático de teste e análise das comunicações com o cartão, desenvolver e implementar um protótipo de solução para o que nos tínhamos proposto no início dos trabalhos. De referir que existiu uma particular atenção em integrar as várias fases da personalização do Cartão U.PORTO num único interface, com a menor dependência possível de bibliotecas de entidades terceiras.

Conseguimos ainda, criar um protótipo de aplicação, que retira proveito da autenticação do utilizador através do seu Cartão de Cidadão, para desta forma realizar uma transferência do não repúdio do ambiente de execução da aplicação para a geração das chaves no seu Cartão U.PORTO.

A arquitetura implementada, permite ainda a convivência de vários tipos de certificados digitais no mesmo cartão, disponibilizando às aplicações necessárias os mecanismos para a sua publicação, arquivo e gestão, possibilitando assim à U.PORTO dispor de mais um serviço para disponibilizar à comunidade académica, permitindo promover a utilização da assinatura digital, autenticação e cifra.

Apêndice A - Utilização Cartão U.PORTO

Ambiente Windows

A utilização do Cartão U.PORTO em ambiente Windows depende da instalação do *middleware* Classic Client produzido pela Gemalto (Ilustração 30 – Aplicação classic cliente). Esta aplicação permite uma interface gráfica para a realização de algumas operações no cartão.

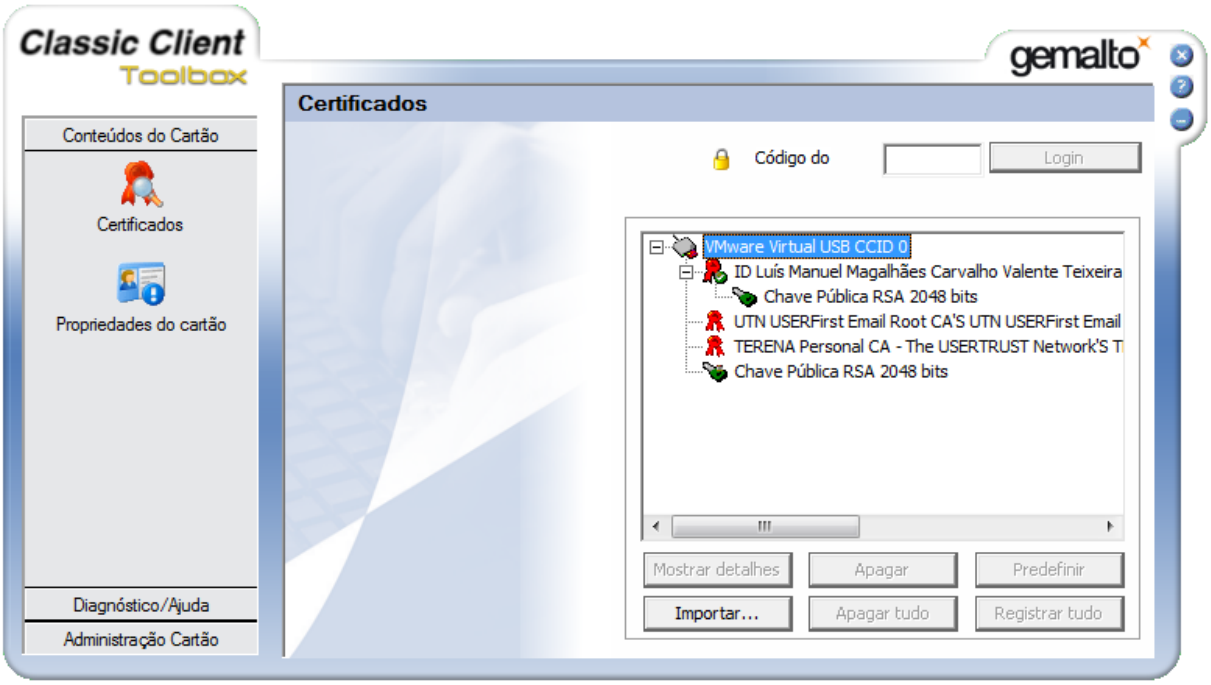


Ilustração 30- Aplicação Classic Client

Para a sua utilização nas ferramentas Microsoft, Google Chrome e Adobe Acrobat não é preciso realizar mais ações, pois o *middleware* regista o dispositivo *smart card* na gestão de certificados do Windows e utiliza a interface CSP para comunicar com o cartão.

No Mozilla Firefox, é necessário adicionar um novo dispositivo de segurança, configurando para o efeito o interface PKCS#11 do *middleware*.

Abrir o Firefox e no menu Ferramentas escolher as Opções.

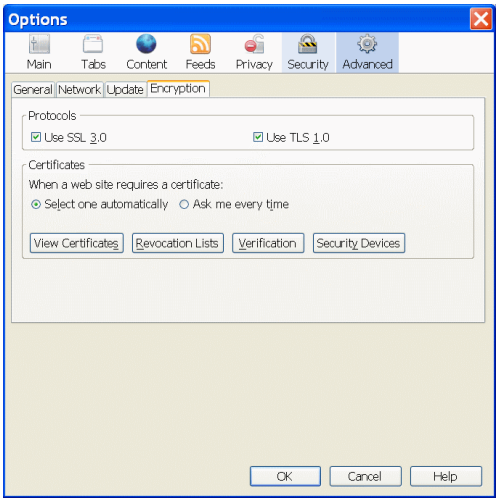


Ilustração 31 - Opções Firefox

Clicar no ícone Avançadas, seguidamente o separador Encriptação, Dispositivos Segurança.

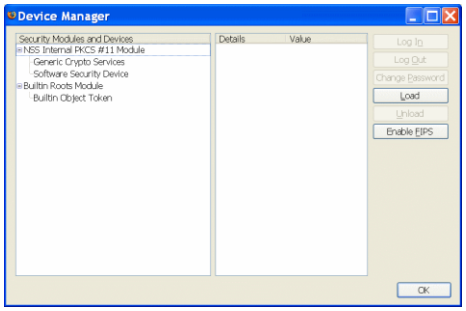


Ilustração 32 - Dispositivos Segurança

Seguidamente, clicar na opção Carregar e configurar as opções com as seguintes indicações.

- Nome Módulo: Cartão U.PORTO

- Ficheiro Módulo: gclib.dll

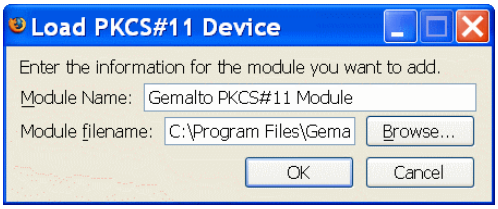


Ilustração 33- Carregamento do módulo PKCS#11 em Windows

Ambiente Linux

A utilização do Cartão U.PORTO em ambiente Linux depende da instalação do *middleware* Classic Client produzido pela Gemalto e só é compatível com a distribuição Ubuntu. Esta aplicação só permite ter uma interface gráfica para a mudança de códigos PIN, sendo bastante mais limitada em funcionalidades, que a versão Windows.

As aplicações mais usuais são configuradas diretamente nas suas opções, sendo idênticas ao exemplo do Mozilla Firefox.

A única diferença para a versão Windows, está no nome da biblioteca a carregar. Sendo utilizadas as seguintes definições.

Após aceder à opção Carregar dispositivo PKCS#11 e configurar as opções com as seguintes indicações.

- Nome Módulo: Cartão U.PORTO

- Ficheiro Módulo: gclib.so

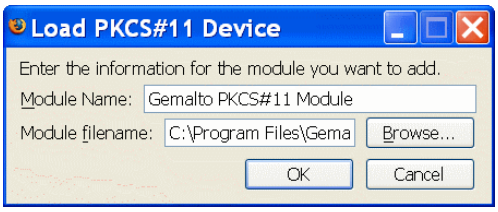


Ilustração 34- Carregamento do módulo PKCS11 em Linux

Apêndice B – Pedido de um certificado pessoal

1. Para solicitar um certificado, o utilizador terá que aceder à aplicação Confusa através do URL: https://tcs-personal.up.pt. Após se autenticar com as suas credenciais da federação RCTS AAI, acedendo à opção "Os meus certificados" terá acesso ao ecrã de pedido de certificados, tal como é visualizado na seguinte ilustração.

Ilustração 35 -Autenticação do utilizador com o CC

Após selecionar o leitor de cartões onde se encontra o Cartão de Cidadão, o utilizador pode autenticar-se, clicando na opção "Cartão de Cidadão."

2. Após a autenticação do utilizador, surge no interface a indicação do utilizador que se encontra autenticado na aplicação, e torna-se disponível o botão para validação do Cartão Universitário - Ilustração 36.

Ilustração 36- Validação Cartão Universitário

3. Validando o Cartão Universitário, surge uma mensagem informando o utilizado que o cartão é válido e permite-lhe definir o código PIN que deseja personalizar no cartão - Ilustração 37.

Ilustração 37- Definição código PIN do utilizador

4. A definição do código PIN no Cartão U.PORTO, se realizada com sucesso, permite ao utilizador solicitar os certificados digitais - Ilustração 38.

Ilustração 38- Pedido de Certificado

5. Após realizar o pedido do certificado, o utilizador é encaminhado para uma página para confirmar que o pedido se encontra correto. Aí é feita a verificação do CSR – Ilustração 39.

Ilustração 39- Verificação do CSR

6. Confirmando o pedido, o utilizador é encaminhado para a página com informação sobre os certificados solicitados, surgindo-lhe a opção para instalar no cartão, os certificados já assinados pela Comodo. Nesta página, a *applet* solicita ao utilizador a indicação de qual leitor de cartões deseja utilizar e a indicação do código PIN que irá utilizar para importar o certificado. No final da operação, o utilizador é informado que o cartão está personalizado - Ilustração 40.

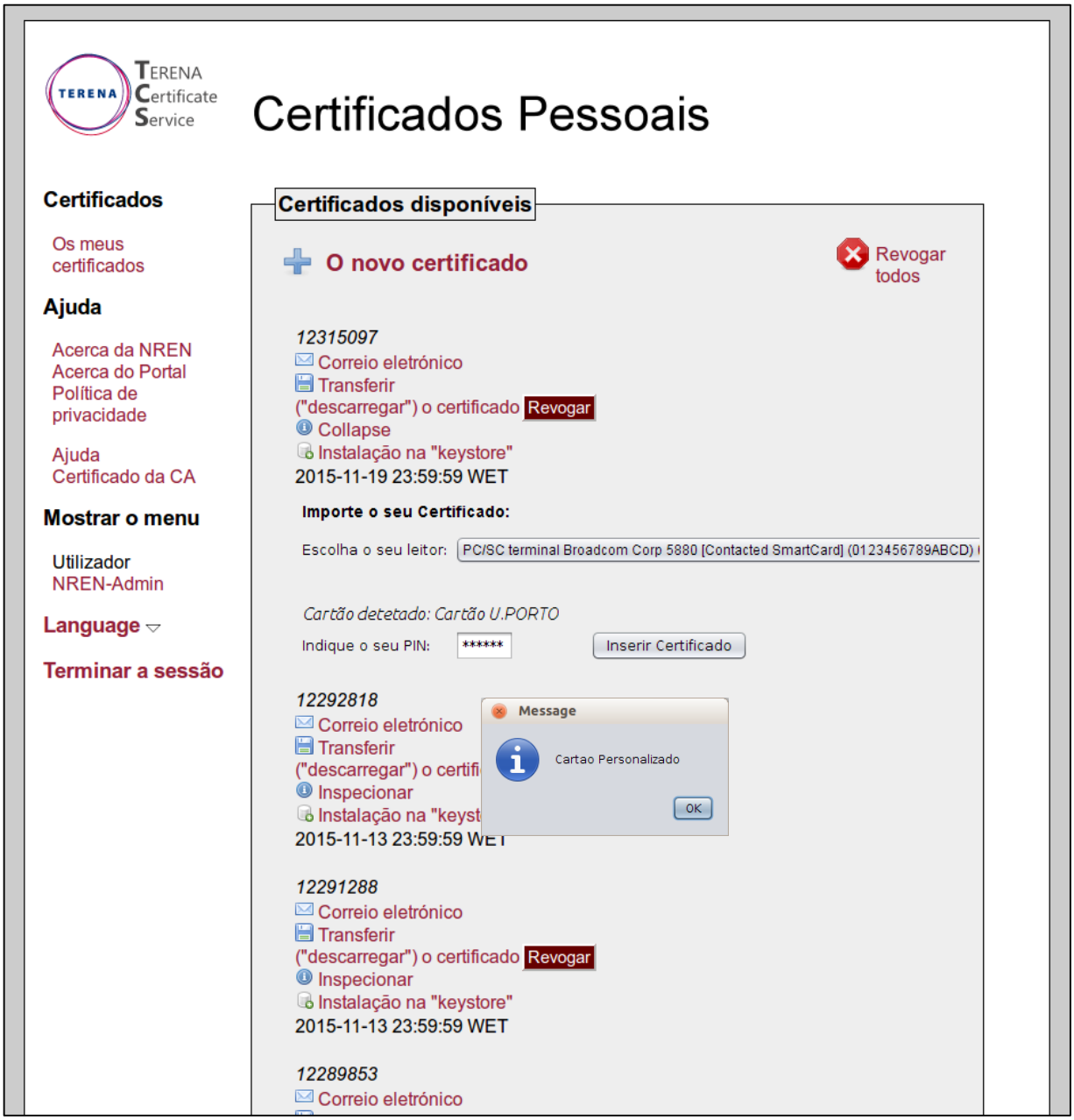


Ilustração 40- Personalização do cartão com o Certificado

Referências bibliográficas

1. Liliana Ávila, Leonor Teixeira, and P. Almeida, *Desmaterialização de processos com recurso a tecnologias open-source numa instituição de ensino superior*, in *CAPSI 2012*2012: Braga, Portugal.
2. Estado Português, P.C.d.M., *Resolução do Conselho de Ministros*, in *109/2009*02-10-2009: Diário da Republica.
3. Frank Pimenta, Cláudio Teixeira, and J.S. Pinto, *Privacy concerns on a Federated Identity Provider Associated with the Users' National Citizen's Card*, in *2010 Third International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies and Services*2010.
4. Uwe Hansmann, M.S.N., Thomas Schäck, Achim Schneider, Frank Seliger, *Smart Card Application Development Using Java*. 2nd ed. 2002.
5. Mayes, K.E. and C. Cid, *The MIFARE Classic story.* Information Security Technical Report, 2010. **15**(1): p. 8-12.
6. Maria, M.D., *Calypso - a smart card for simplyifing the city life.* 1999.
7. Burr, W.E., D.F. Dodson, and W.T. Polk, *Electronic Authentication Guideline*, 2006, National Institute of Standards and Technology
8. Liu, J. and L. Vigneron, *Design and verification of a non-repudiation protocol based on receiver-side smart card.* Information Security, IET, 2010. **4**(1): p. 15-29.
9. Portuguesa, R., *Regime jurídico da assinatura digital*, 2006: Diário da República.
10. Zhu, X. and X. Lu. *Research on Backup and Recovery of Key Mechanism of PKI*. in *Intelligent Systems and Applications, 2009. ISA 2009. International Workshop on*. 2009.
11. Johan Ivarsson, A.N., *A Review of Hardware Security Modules*, 2010, Certezza AB Stockholm. p. 31.
12. Allan, A., *Magic Quadrant for User Authentication 2011*, 2012, Gartner.
13. Agência para a Modernização Administrativa, I. *Estatísticas - Cartão de Cidadão*. 2012 [cited 2012 Setembro 2012]; Available from: http://www.cartaodocidadao.pt/index.php?option=com_content&task=view&id=295&Itemid=26&lang=pt.
14. RSA Laboratories, *PKCS #11: Cryptographic Token Interface Standard*, 2001.
15. Sanchez-Martinez, D., et al., *Towards e-Government: The security SOA approach of the University of Murcia.* 2008. **-**(-): p. - 818.
16. Cádiz, U.d., *Reglamento de la Tramitación Telemática de Procedimientos en la Universidad de Cádiz*, in *REGLAMENTO UCA/CG05/2010*, U.d. Cádiz, Editor 2010: http://www.uca.es/web/serviciosdigitales/ae/normativa.
17. Almería, U.d., *Normativa de Registro de la Universidad de Almería*, 2007: http://cms.ual.es/UAL/administracionelectronica/normativa/index.htm.
18. Halawani, T. and M. Mohandes, *Smart card for smart campus: KFUPM case study.* 2003. **- 3**(-): p. - 1255 Vol.3.
19. Jianwen, F., L. Feng, and L. Xuan, *Current situation and development of China Campus Card System.* 2010. **-**(-): p. - 474.
20. Mirza, A.A. and K. Alghathbar. *Acceptance and Applications of Smart Cards Technology in University Settings*. in *Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on*. 2009.

21. M. Arami, M.K., and, R. Krimmer. *User Acceptance of Multifunctional Smart Cards*. in *13th European Conference on Information Systems*. 2004. Turku, Finland.
22. Chung-Huang, Y., *On the design of campus-wide multi-purpose smart card systems.* 1999. **-**(-): p. - 468.
23. Liu, C., Z. Xie, and P. Peng. *A Discussion on the Framework of Smarter Campus*. in *Intelligent Information Technology Application, 2009. IITA 2009. Third International Symposium on*. 2009.
24. Komar, B., *Windows Server® 2008 PKI and Certificate Security*. 2010: Microsoft.
25. *EJBCA: The J2EE Certificate Authority*. 09-2012]; Available from: http://www.ejbca.org/.
26. Cooper, D., et al., *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Internet Engineering Task Force (IETF)
27. Internet Engineering Task Force, *RFC 2560 - Online Certificate Status Protocol - OCSP*, 1997.
28. Ghori, A.I. and A. Parveen, *PKI administration using EJBCA and OPENCA* 2006, George Mason University.
29. *EJBCA - Hardware Security Modules (HSM)*. 09-2012]; Available from: http://www.ejbca.org/adminguide.html#Hardware Security Modules (HSM).
30. Standardization, I.O.f., *ISO 7816-4 Smart Card Standard: Part 4: Interindustry Commands for Interchange*, 2005.
31. Standardization, I.O.f., *ISO/IEC 7816-3:2006 Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*, 2006.
32. Standardization, I.O.f., *ISO/IEC 14443-2:2010 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface*, 2010.
33. Standardization, I.O.f., *ISO/IEC 14443-3:2011 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision*, 2010.
34. Standardization, I.O.f., *ISO/IEC 14443-4:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol*, 2008.
35. RSA Laboratories, *PKCS #15: Cryptographic Token Information Format Standard*, 2000.
36. Europeia, C., *Diretiva 1999/93/CE* 1999.
37. Internet Engineering Task Force, *The Transport Layer Security (TLS) Protocol, Version 1.2*, 2008.
38. Internet Engineering Task Force, *HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)*, 2007.
39. Song-Kong, C., C. Shu-Fen, and H. Min-Shiang. *A simple method to secure the integrating a key distribution into digital signature standard*. in *Computing Technology and Information Management (ICCM), 2012 8th International Conference on*. 2012.
40. Basin, D., P. Schaller, and M. Schläpfer, *Web Application Security*, in *Applied Information Security*. 2011, Springer Berlin Heidelberg. p. 81-101.
41. Hope, P. and B. Walther, *Web Security Testing Cookbook*. 2008: O'Reilly Media, Inc.
42. X.509, I.-T.R., *Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks* 2005.
43. RSA Laboratories, *PKCS #12: Personal Information Exchange Syntax Standard*, 1999.
44. Oracle. *Java ™ Cryptography Architecture (JCA) Reference Guide*. 2012; Available from: http://docs.oracle.com/javase/7/docs/technotes/guides/security/crypto/CryptoSpec.html.

45. Initiative, I.M., *Initiative, Internet2 Middleware. "Shibboleth."*, 2011, Internet2 Middleware Initiative.