# CV-TTFJ

Embedded Software Engineer – Cryptography

## Work Experience

**TECH TEAMZ | August 2023 – Currently**

**Cybersecurity and Cryptography**

Role: Team Lead, Software Architect, Senior Developer, Tester

Main Tasks:

Development of high-quality security software products from embedded devices to cloud systems; design, implement, test, review, document, and debug as a member of our agile development team; give estimates on new features and their influence on system design; participate in product road mapping process and plan development tasks and related activities; and investigate and resolve customers support tickets.

Core Skills: C, C++, cryptography algorithms, (AES, 3DES, RSA, ECC), TLS, OpenSSL, SDKs, Scrum/Agile, Linux, Windows, SonarQube/SonarLint, CppUnitTest Framework.

---

**NEURALLABS | November 2022 – August 2023**

**Cybersecurity and Cryptography**

Role: Software Architect, Senior Developer, Tester

Traffic Analytics

Main Tasks:

Leading the Edge Product Development, in charge of design, implement and test the libraries that manages the engine of the Camera for recognizing license plates, vehicle brand, vehicle color, etc.... The solution works for different camera brands as Vivotek, Axis, Zkteco. Development using C++ 14. Multiplatform code to make easier the integration testing (simulation environment) using Windows and Linux OS. Using SonarQube/Sonar Lint to assure the code quality. Unit Testing with CppUnitTest FrameWork

Core Skills: C++ 14, Linux Debian, Linux Ubuntu, TCP/IP, CGI

Tools: MS VS 2022, AzureDevOps, Git, Vagrant, SonarQube, VirtualBox, Doxygen Security staff: AES, 3DES2K

---

**EXPLEO GROUP | March 2021 – November 2022**

**Railway Transport**

Role: Project Manager, Team Lead, Software Architect, Senior Developer, Tester

Main Tasks:

- Leading a Railway Project in charge of design, implement and test the following libraries for the RBC platform of a Railway Spanish Company:
    - SUBSET-037: EuroRadio FIS. Communication Protocol Onboard - Track Devices
    - SUBSET-098: RBC-RBC Safety Communication Interface
    - SUBSET-114: KMC-ETCS Entity Offline Key Manager
    - SUBSET-137: On-line Key Management
    - RaSTA (RailSafe Transport Application) Protocol
    - Communications Manager in charge of manage the different connections used by the
    - RBC platform, running under ARM boards with a topology of 2oo3 for the application side and two redundant transport boards.
- Development using C++ 11 under EN-50128 rules.
- 100% of Code Coverage required using VectorCast as unit testing tool.
- Multiplatform code to make easier the integration testing (simulation environment) using
- Windows and Linux OS.
- Using SonarQube to be compliance with MISRA C++ 2008.
- IBM Rhapsody used for build the Architecture, Design and Implementation deliverables to the client. Generate the requirements with the client and integrate them using IBM Workflow Management.

Security activities:

- Implement in a secure way the symmetric cryptographic algorithms required (AES256, 3DES2K)
- Configure the PKI and PSK modes for the TLS Server using OpenSSL required to
- parse messages from the Key Manager Center
- Store in a secure way in NVM the keys configured for the device
- Securitized a proprietary protocol to communicate devices in a local network
- Define the Security Architecture with the client
- Manage the OpenSSL API to be able to use protocols like CMP and OCSP

Technologies: C++ 11, Boost, OpenSSL, LwIp, Linux Ubuntu, TCP/IP

Tools: MS VS 2019, GitHub, RedMine, IBM Rhapsody, SonarQube, VectorCast

Security staff: OpenSSL, TLS, CMP, OCSP, PKI, PSK, AES, 3DES2K

---

**EXPLEO GROUP | November 2019 – March 2021**

**Railway Transport**

Role: Senior Java Development Engineer

Main Tasks:

Java Web Server development running under a Linux device, for software update of different elements of the railway system.

Security activities:

- Implement a solution to be able to store in a secure way the certificates used by Nginx
- Use and customize if required the BouncyCastle Java Library to be able to sign and encrypt XML used
- In charge of maintain the Security Library of the Server to give services of encryption, sign, verification, manage of certificates
- Configuring the certificates of Nginx and maintain the PKI tree
- Define the Security Architecture with the client

Technologies: Java 8/11, Maven, MariaDB, Linux, OPC UA, Junit, Mockito, Jax-RS, Jetty, Hibernate, Nginx, Java FX, PostgresSQL

Tools: Eclipse, GitHub, Jenkins, Trello, SonarQube, MS Visio, jMeter Security staff: BouncyCastle, PKI, TLS, XML sign and encryption, KeyStore

---

**INDRA SYSTEMS | Octubre 2019 – Noviembre 2019**

**Terrestrial Transport**

Role: Senior Development Engineer

Main Tasks:

Maintenance of Java and C# applications running under a Linux device, located inside informative panels (showing estimation times) at buses stops

Technologies: Java, C#, Shell, Spring, Maven, SQL

Tools: Eclipse, GitHub, SVN, JIRA, Trello, SonarQube, MS Visual Studio

---

**VALID SOLUCIONES TECNOLÓGICAS SA | February 2017 – February 2019**

**Telecommunications, SmartCards**

Role: Technical Lead & Scrum Master for eUICC project

Main Tasks:

Leading a team of 6 firmware developers With Project Manager and Product Marketing Manager:

- Identify the requirements of the client
- Defining the deadliness for the tasks
- Setup the Sprint for create a deliverable iteration With Developers Team:
- Identify the task and the responsible of the execution
- Lead the Scrum daily meetings - Facilitator, avoiding dead spots in the tasks
- Get feedback from developers, to improve next iterations Acting as Senior Developer Engineer as well (see the previous position)

Security activities:

- Certificate the security of the 5G encryption algorithm implementation (Certificate obtained with BrightSight laboratories)
- Security Architecture definition to assure the key assets of the client (Vodafone)
- Design and Implementation of a Security Platform located in the Kernel of the OS to protect the data managed by the JCRE
- Use of a ST33 device with crypto CPU and follow the security guidelines of the manufacturer and the smart card industry

Technologies: C,C++, JavaCard, Java, Phyton, IOT, eUICC

Tools: Keil, Eclipse, NetBeans, GitHub, AccuRev, JIRA, Trello, SonarQube, MS Visio
Security Staff: ST33 Crypto device, JavaCard Security Platform, ECCs, RSA, DES, AES

---

**VALID SOLUCIONES TECNOLÓGICAS SA | February 2009 – February 2017**

**Telecommunications, SmartCard**

Role: Senior Firmware Developer Engineer member of the Innovation-Low Level group inside RnD Department

Main Tasks:

- Analysis, Development and Testing of the Operating System Core
- uVision configuration, Keil Tools, compiler options.
- Development in C language for ARM 32 bits and Intel 16 bits CPUs
- Wide knowledge in NVM FLASH memory handle
- Memory Management - Transaction mechanism
- Anti-Tearing mechanism
- Communications (ISO, SWP)
- Algorithms HW&SW
- Functionalities optimization
- Knowledge and use of Doxygen (C code documentation)
- Knowledge in SonarQube for C language Wide experience in development under ST, Samsung and Infineon CPUs of 16 and 32 bits and EEPROM FLASH memory.

Security activities:

- Analysis, Development and Testing of the Operating System Core for JavaCard Banking Card with VISA and Mastercard’s applications

- EMV certification obtained Analysis, Development and Testing of the Operating System Core for SIM NFC JavaCard with VISA, AMEX and MasterCard applications
- RSA algorithm secure implementation
- Implementation of SWP/HCI communication protocol (to support NFC for SimCards)
- Implementation of the core following security guidelines from EMV and SimCard manufacturers.
- Development of code protected against different attacks (double fault, fault injection…)
- Certification process with UL laboratories
- GlobalPlatform certification obtained Analysis, Development and Testing of the Operating System Core for embedded SIM JavaCard
- ECC algorithm secure implementation
- Testing using Java Tools and BouncyCastle library
- Assistance to standardization committees \ SIMAlliance \ GlobalPlatform (conference calls)

Technologies: C, C++, JavaCard, Java, NFC, ARM/Intel

Tools: Keil, NetBeans, AccuRev, JIRA, SonarQube, Doxygen Security Staff: ST33 Crypto device, JavaCard Security Platform, ECCs, RSA, DES, AES

---

**SANDISK | October 2007 – February 2009**

**Telecommunications, SmartCards, Mobile Applications, Flash Memory**

Role: Firmware Developer Engineer

Main Tasks:

Analysis, Development and Testing of SlotRadio application for different mobile platforms (RIM & J2ME). Collaborating with a Team allocated in Israel, helping to release a first version of this music player

Technologies: RIM, J2ME.

Tools: Eclipse, AccuRev, JIRA, MS Project.

---

**M-Systems Ltd | October 2006 – October 2007**

**Telecommunications, SmartCard, Flash Memory**

Role: Firmware Developer Engineer

Main Tasks:

Project megaSIM :

Develop a SIM OS in an embedded device with 1Gb of FLASH storage capacity and SmartCard capabilities. TCP/IP protocol stack implementation for SIM JavaCard Operating System.

Technologies: C, JavaCard, Java, FLASH memory, TCP/IP

Tools: Keil, AccuRev, JIRA

---

**MICROELECTRÓNICA ESPAÑOLA | November 2005 – October 2006**

**Telecommunications, SmartCards**

Role: Firmware Developer Engineer

Main Tasks:

- Analysis, Development and Testing following standards of ETSI, GSMA...
- Implementation in C code for SmartCard devices with EEPROM memory
- Application development following standards: \ BIP (Bearer Independent Protocol) \ SAT \ WIB maintenance \ CATRE (Card Application Runtime Environment) maintenance
- Application Testing: \ Proprietary scripts development \ Standard Testing scripts development in Java J2EE \ Library for Testing Tools development in Java J2EE
- JavaCard Applets development for testing

Technologies: C, JavaCard, Java, EEPROM memory, SmartCards, ARM/Intel architectures

Tools: Keil, Tortoise

---

## STUDIES

Computer Engineering - Universidad Pontificia de Salamanca, Madrid (2002-2005).