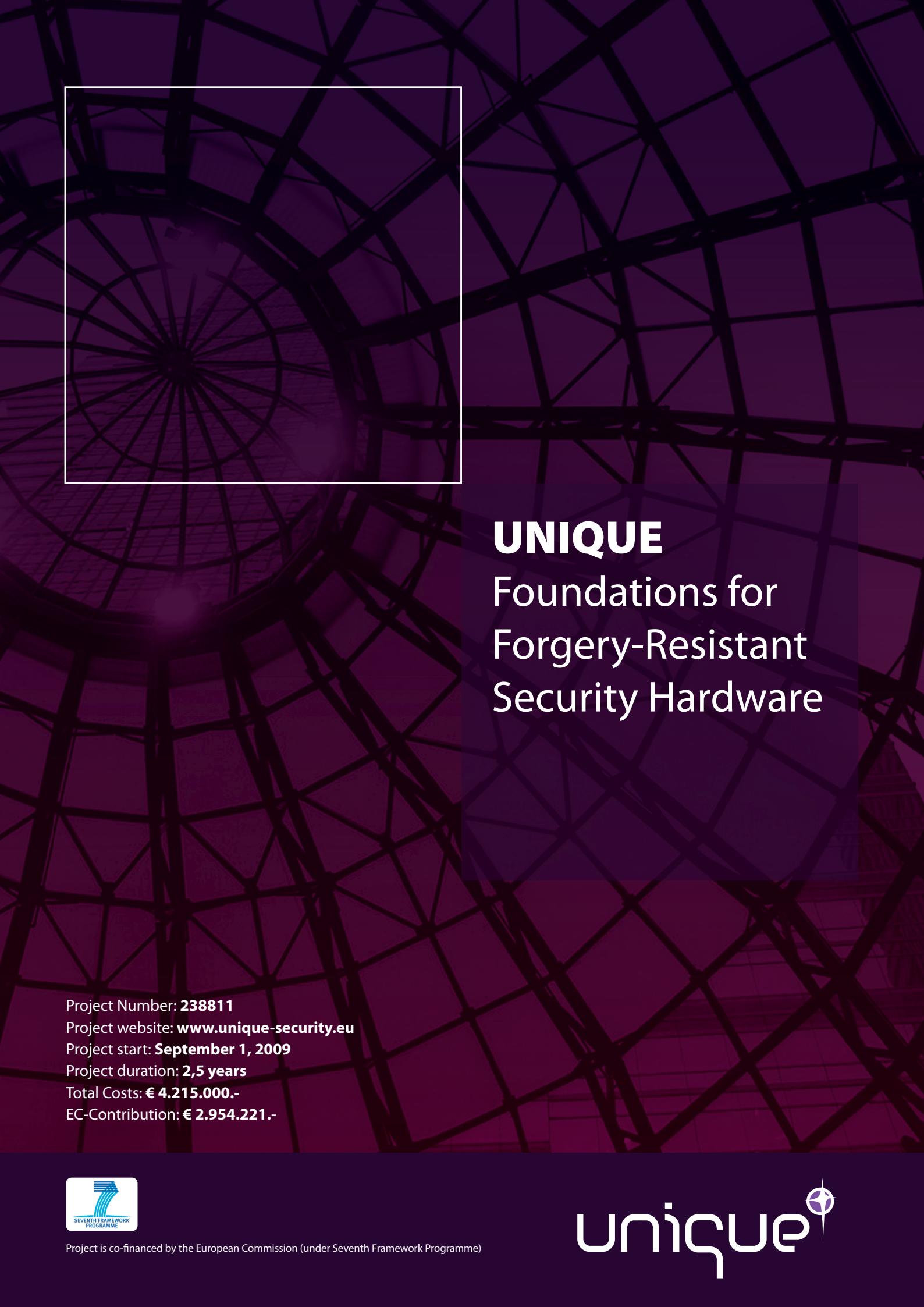


UNIQUE

Foundations for Forgery-Resistant Security Hardware

Project Number: **238811**
Project website: **www.unique-security.eu**
Project start: **September 1, 2009**
Project duration: **2,5 years**
Total Costs: **€ 4.215.000.-**
EC-Contribution: **€ 2.954.221.-**

Project is co-financed by the European Commission (under Seventh Framework Programme)

Mission of UNIQUE:

Mission of the project is to enforce the security and assurance of hardware components against malicious attacks of unauthorised parties.

Motivation:

Counterfeiting of goods and Intellectual Property (IP) has reached a level that threatens industrial production, organisational function, health systems and even national security when malicious elements are deployed for critical infrastructures.

Nearly every industry area is using hardware chips to adopt security issues. In future the pharmaceutical area will use Integrated Circuit (IC) chips in the packaging material to prevent patients from taking faked. This problem can be avoided by using unclonable ICs in order to be able to clearly identify genuine drugs.

Counterfeiting can damage the benefit and also the brand of legitimate producers so this would be a substantial loss for the supplier. The need of architectures which offer higher security in all kinds of hardware components is present. By using such innovative approaches the prevention of counterfeiting and the protection of IP will be enhanced.

The development of these structures is still in its infancy and so the UNIQUE project will focus on its growth.

unique

Objectives:

The UNIQUE project tends to increase the protection of hardware systems against the following security vulnerabilities:

- Counterfeiting
- Cloning
- Tampering
- Reverse engineering and
- Insertion of malicious components.

In UNIQUE hardware-based cryptography and security building blocks, security architectures, protocols, algorithms, design and evaluation principles will be combined to mainly enhance embedded hardware components with security functionalities.

The goal of the UNIQUE project is to develop solutions to the counterfeiting problem. These solutions need to be supported by strong, novel and consistent design and evaluation methods that have to ensure the security on each different levels.

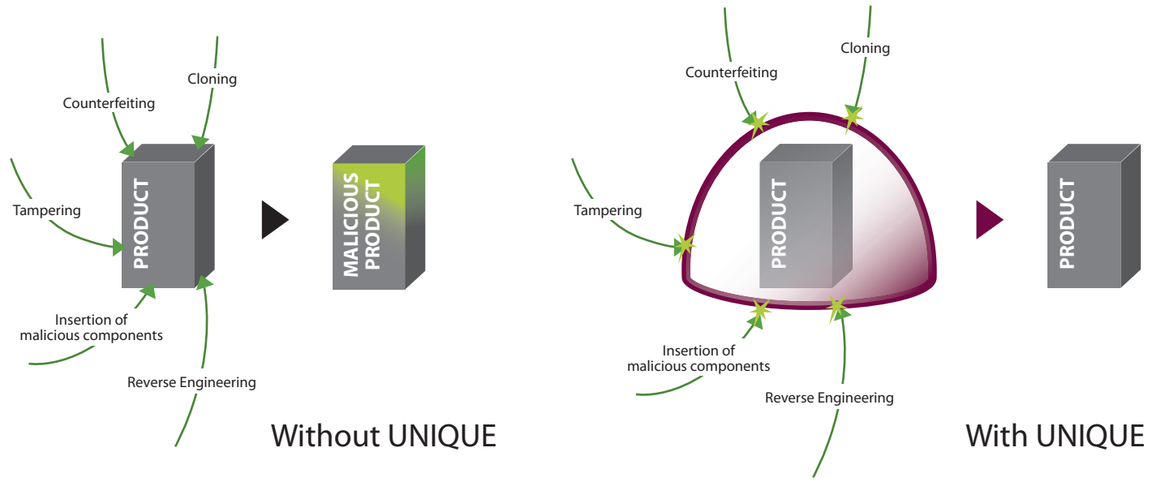
- Application and deployment level: counterfeiting, verifiability, auditability and detection of malicious hardware.
- Design and implementation level: sub-micron physical security primitives (primarily Physically Unclonable Functions, PUFs) and entanglement of cryptography and physics.
- Evaluation level: cryptographic and security framework.

Overall Strategy:

First Year: Identification of requirements, threat models and building blocks.

Second Year: Novel methodologies are listed, described and designed, enhancement of approved structures.

Last Half Year: Test framework design, implementation, integration of the prototype and evaluation.



Technical Approach:

The development of the UNIQUE project is organised in four technical work packages as well as two work packages for Dissemination and Project Management:

WP1: Requirements, Design and Evaluation: focuses on the identification of the threat model(s) and analysis hardware building blocks. It also identifies the security design and evaluation methodologies for hardware anti-tampering and anti-counterfeiting solutions.

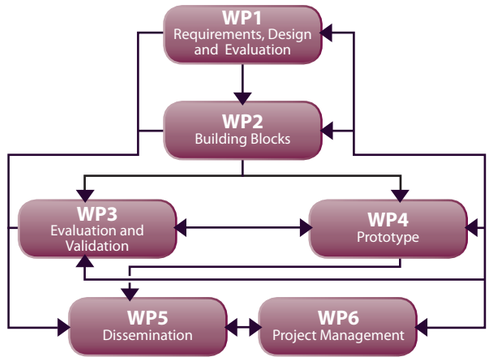
WP02: Building Blocks: develops PUFs and combines them with cryptographic primitives.

WP03: Evaluation and Validation: points at the methodology and practice of evaluation and validation of the novel result.

WP04: Prototype: Proof of concept for the innovative achievement.

WP05: Dissemination: Coordinated management of dissemination and exploitation for the UNIQUE project in order to enable maximum impact on the European security market.

WP06: Project Management: Effective operational management with regard to contractual, financial, legal, technical, administrative and ethical management issues.



Project Results and Innovation:

The UNIQUE project will develop innovative concepts to make the state of the art of ICs and hardware components that provide cryptographic and security services more secure:

Emerging technologies and innovation: In UNIQUE the new concept of the PUFs will be used to design novel hardware labelling and authentication mechanisms.

Innovation: New hardware products with an enhanced assurance and security against counterfeiting and tampering can be developed by the novel tools, methodologies and principles. The UNIQUE project will step forward particularly in the application areas such as consumer electronic, automotive and avionic and pharmaceutical industries, critical infrastructures as well as governmental use.

The most innovative aspect of the UNIQUE project is that the security of the explored primitives is implemented on physical instead of computational modules.

unique

Contact:

Project Coordinator
Klaus-Michael Koch
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
9500 Villach
Austria
Tel.: +43 4242 233 55 – 0
Fax: +43 4242 233 55 – 77
E-mail: coordination@unique-security.eu
Web: www.unique-security.eu

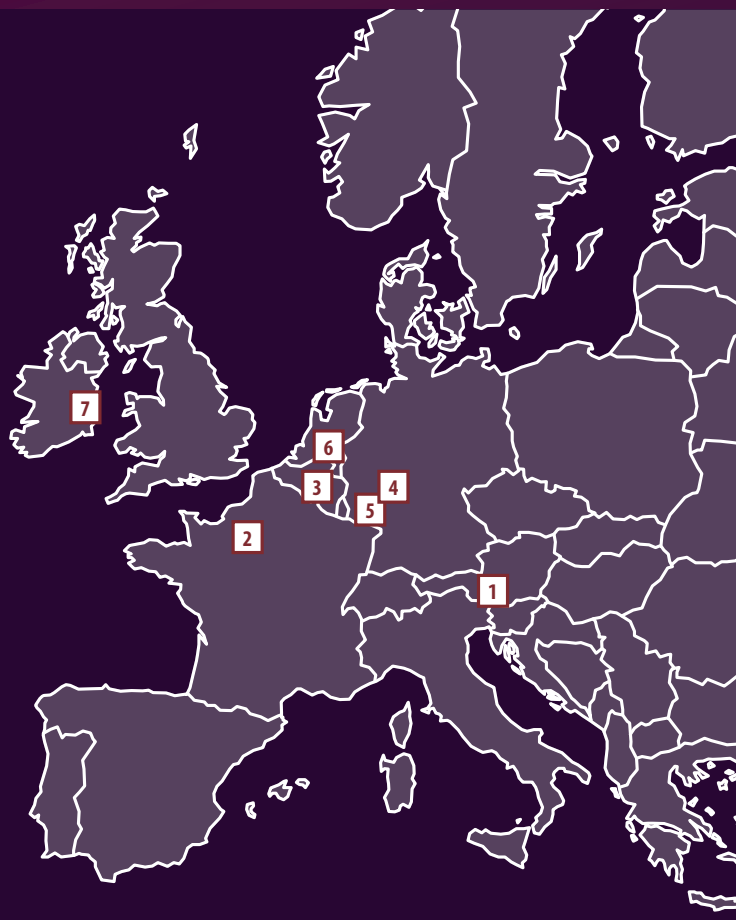
Technical Project Leader
Pim Tuyls (Intrinisic-ID)

Scientific Project Leader
Ahmad-Reza Sadeghi (TU Darmstadt)

Project Management Leader
Martina Truskaller (Technikon)

Consortium:

The UNIQUE consortium consists of two universities and five companies from six European countries (Austria, Belgium, France, Germany, Ireland and the Netherlands). The expertises of the companies range from deep skills in security products to the development of the architectural structure of test frameworks to the full development of PUFs and a general high competence in the Information Technology. The universities bring along the ability of requirement engineering, the know-how on needed hardware components, the development of secure cryptographic algorithms and protocols and the possibility to make performance and security tests.



Project Partners:

The consortium is constituted of 7 partners from 6 different countries:

1 **Technikon Forschungs- und Planungsgesellschaft mbH (Austria)**

2 **Thales Communications (France)**

3 **Katholieke Universiteit Leuven (Belgium)**

4 **TU Darmstadt (Germany)**

5 **Sirrix AG (Germany)**

6 **Intrinsic-ID (Netherlands)**

7 **Intel Performance Learing Solutions Limited (Ireland)**