Security Architect

Name & Address	Wim Ton Geaglom N41 DX63 Drumkeeran mobile +353 89 4965841 E-mail: wimton@yahoo.com	
Citizenship of:	The Netherlands, eligible to work in all EU countries	
Summary:	Experienced architect for PKI, key management, and device personalization, mainly in the field of IoT Expert in formal device security certification, mainly CC, Metas, FIPS-140, CPA Correct implementation of cryptography.	
Professional Experience:		
July 2021 TrustCB	Common Criteria Certifier: - Supervising Common Criteria (ISO-15408) certifications -	
Apr. 2011 – July 2021 Landis + Gyr	Security Architect: - Internal security consulting. - Architecting security enhancements for existing products - Common Criteria (ISO-15408) and Metas certifications. - Designing and implementing Key management and PKIs for smart metering. Operating the root CAs (using Thales Luna HSMs) for these PKIs. - Introduction of secure remote firmware update, using an ECDSA signature. - Designing and implementing of personalisation systems for security modules, mainly written in Java. The SCP master keys and the private keys are stored on Thales Luna HSMs. - Design of the symmetric key management of smart meters - Introduction of penetration tests for non-TCP/IP devices - Contribution to smart meter standardisation (UK, CH, DE, EU) - Security modelling for IoT - Member of the product CERT, providing risk assessment and mitigation proposals for the product managers in case of security flaws. - Creating security awareness - Implemented a lean TLS stack for embedded systems.	
Jun. 2010 – Apr. 2011 Secacon	Software developer: - Key management for directory encryption with MFC, PKCS12 and XML - Single-Sign-On with MFC, BHO and PKCS11	
Feb. 2008 – Jun. 2010 PayTec AG	Software developer: - Developing software for payment terminals[1] - Extending the embedded software to comply with PCI security requirements - Achieved PCI-POI certification for the PIN pad software - Achieved Level 2 certification for MasterCard and Visa contactless payment kernels - Project leader of the RFID project.	

[1] SBB,,Valora, Post

	- Design of a CA for software certificates (for remote firmware update)
Mar. 2006 – Feb. 2008 Belos AG	Microsoft Navision/Dynamics Developer: - Maintenance and extension of the ERP system for Brack /Alltron electronics using agile methods - Factoring and stock management system for Zusa..
Dec. 2004 –Mar. 2006 Contracting	Various projects for among others NXP: - Develop standards and applications for contactless smartcards and NFC devices, mainly in the field of Digital Rights Management - Co-author of a patent on the application of RFIDs to protect DVDs - Member of the security commission of the NFC Forum (standardisation comity) - Conducting a workshop about Java smartcard security - Design of a key-management system and security features for a GSM based network of dataloggers with mutually distrusting users.
Apr. 2001-Dec. 2004 Aspects-Software, Edinburgh (UK) (Now NXP)	Senior Software Engineer - Design and implementation of embedded software for smartcards, written in a mixture of C, C++, Java, and assembler in a team of 6 developers. - Achieved FIPS-140 Level 2 approval for the OS755 smartcard OS. - Speeded up the generation of RSA keys by 400%[2] while reducing code size and increasing speed. - Educating my work colleagues in the proper use of security and cryptography. - Design and implementation of a SIM card. - Implementation of a Perl program to compress Java byte code by 20% and extending the VM to accept the new compressed instructions. - Member of the ETSI standardisation comity on smartcards
Nov.1989 – Apr. 2001 NLNCSA (the Dutch NSA), Den Haag. (NL)	Software Engineer /Security consultant - Design and verification of computer security and crypto-equipment, consultancy for computer and communications security. - Build and deployed a key generation system, to produce high quality random and prime numbers. Writing drivers for the custom random number hardware. - Build and deployed a key management system for an army wireless network. - Achieved NATO certification for a secure radio system. - Designed and supervised the construction of a B1 (Orange Book) operating system written in C and C++.
Sept.1984 – Nov.1989 Pink/Roccade, Zoetermeer (NL)	Helpdesk employee at Shell Oil in Assen: - Supporting 1500 users on MS-DOS PCs with Novell Netware, on VAX/VMS and on IBM VM/CMS. Writing documentation in SGML.
Sept.1983 – Sept.1984 Dresser Atlas, (USA, UK, NL)	Well-logging engineer: - Geophysical measurements (among others with γ and neutron sources) and maintenance of gas-wells with instruments or explosives suspended on a very long wire
1982 - 1983 KISC Kandersteg	Volunteer at Kandersteg International Scout Centre: - Designed and supervised the extension of a youth hostel, also working as a cook and mountain guide
Aug. 1980 –	Programmer-analyst for numerical mechanics programs, Basic on HP1000

[2] Using Pommerance's observations on the distribution of pseudo-primes

Mai.1982 HTS Den Bosch	
1977 Bos Kalis	Concrete designer in Hassi r'Mel, Algeria
Education:	- Mathematics and cryptology from the Open University - Bachelor in InformationTechnology from AMBI in Maarssen - Masters degree in civil engineering, specialisation in numerical mechanics from Delft University of Technology
Courses	Mathematics at the Open University • Cryptography • Error correcting codes • Algebra • Discrete mathematics • Formal languages and automata theory • Microprocessor architecture Others • PCI –PED • Common Criteria introduction • Formal methods in program verification (BAN, CSP, Isabelle) • Project management • C++ • DSPs and FPGAs
Other skills:	- Usable developer skills for : Java, C, C++, C#, XML, ASN.1 - Digital electronics - Microsoft Windows, Office, Linux, and some Git.

Languages:	**Oral:**	**Written:**
English	- Fluent	- Very good
German	- Good	- Good
Dutch	- Fluent (Mother-tongue)	- Very Good
French	- Good school knowledge	- Good school knowledge

Hobbies:	Climbing, skiing, running, electronics, ham radio EI4VYI
Driving:	I have a full, clean licence and I own a car.