

brightsight®



your
partner
in security
approval



Security
Training by the
Specialists

Brightsight

training courses – spreading security around the globe

The value of knowledge on the credit side of our activities' balance sheet is extremely high and becomes manifested in the hundreds of security evaluation projects we have carried out. On the one hand, it is reflected in the development of innovative test methodologies and tools. On the other hand, we transfer this unique expertise to our customers in comprehensive training courses and workshops in order to equip them effectively for the challenges in the area of smart card security, payment device security and Common Criteria evaluations.

Common Criteria for Developers

Course objectives

- Essence of Common Criteria (CC)
- The basics of structure, terminology, content and application of CC
- Requirements and consequences for obtaining a CC certified product

Services

- Brightsight Certificate of Attendance
- Course manual

Program

Day 1 - Essence of Common Criteria

- The CC standard
- The (hidden) structure of the CC standard and how it is actually used
- Various roles in the CC evaluation and certification
- Recognition and assurance levels
- Summary
- Q & A

Day 2 - The Developer's Practice

- Differences between certification bodies and labs
- Costs and efforts
- The CC history and relation to other standards
- Summary
- Q & A

Unless requested otherwise, examples from the smart card and payment terminal industry will be used throughout the course.

Smart Card Security

Course objectives

- Smart card security from a business and risk point of view
- Smart card security threats
- Smart card security attack techniques
- Generic smart card security techniques
- Smart card security evaluation process

Services

- Brightsight Certificate of Attendance
- Course manual
- Lab tours providing insight in how smart card security is put to the test at Brightsight

Program

Day 1 - The hardware side of smart card security

- Hardware security threats (reverse engineering, mechanical probing, focused ion beam manipulation) with demonstration in the lab
- Perturbation security threats (power and light manipulation) with demonstration in the lab
- Summary
- Q & A

Day 2 - Side-channels and contactless smart card security

- Side-channel security threats (power consumption or electromagnetic emanation on both, hardware and software level)
- Demonstration of side-channel analysis in the lab
- RF ID and contactless smart card security threats (privacy violation, identity theft, virtual pick pocketing) with demonstrations in the lab
- Summary
- Q & A

Day 3 - The software side of smart card security

- Software security threats (most common security threats, resistance against specific OS security threats)
- Commonly known software countermeasures
- Summary
- Q & A

PIN Entry Device and Terminal Security

Course objectives

- The PCI PTS approval program – requirements, evaluation methodology and certification
- Payment terminal security threats
- Payment terminal attack techniques
- General defence mechanisms
- Additional PCI PTS programs

Services

- Brightsight Certificate of Attendance
- Course manual

Program

Day 1 - Security requirements and attack techniques

- Introduction into the PCI PTS security requirements, their intention and how to apply them in practice
- Payment terminal attack techniques and general mechanisms for protection
- Attack potential calculation and how to determine device resistance
- Summary
- Q & A

Day 2 - Global threats and the PCI program developments

- Key management and the impact on PCI PTS compliance
- Side-channel-analysis applied to payment terminals
- Additional security programs of PCI PTS
- Relevant details about the PCI PTS certification process
- Summary
- Q & A

Sharing high-level advisory in latest product security

Our workshops are aimed at industries developing smart cards such as banking, transport, ID or e-passport as well as telecommunications and conditional access industries (Pay TV) and the embedded security industry. Depending on the topics, the groups of participants include risk and fraud managers, marketing and product managers of secure IT products and smart cards, in particular hardware and software developers. On customer request, we also provide individual advanced training programs with more complex contents such as Common Criteria for new schemes, advanced security analysis techniques and more.

The courses will start at 9:00 a.m. and end at 5:00 p.m., including two short coffee breaks and one hour for lunch. All courses take place at the Brightsight office in Delft, The Netherlands.

The courses do not require prior knowledge of CC, smart card or payment device security, although general knowledge of IT security is convenient.

Brightsight Security Training Courses – head start due to knowledge

Take advantage of our extensive expertise and our experience and ensure a profitable competitive edge in product security. As data security is constantly being threatened by new attack techniques, it is of invaluable advantage to continuously protect products and make them future-proof with the valuable backing of knowledge.



Brightsight is your globally recognized partner in security approval of IT products
Security Evaluations and Audits, Training, Consultancy, Tools

delftechpark 1
2628 xj delft, the netherlands
p (+31) 15 269 2500
f (+31) 15 269 2555
info@brightsight.com
www.brightsight.com