Why should cryptographers care about certification?

Dan Bogdanov, PhD

Chief Scientific Officer, Cybernetica

Head of the Standing Committee on Cybersecurity, Academy of Sciences



Welcome to Future Cryptography!

- The goal of the Future Cryptography conference is to promote advances in cryptography that can help remove trust assumptions in systems.
- The conference is co-organised by the Cyber-Security Excellence Hub in Estonia and South Moravia (European Commission CHESS project, grant agreement 101087529), Standing Committee of Cybersecurity of the Estonian Academy of Sciences and Cybernetica.









Certification is the ultimate peer review

Papers			
Cryptographic schemes are	- Standards Researchers	Products	
peer-reviewed by other researchers.	agree that the scheme has the security and performance properties sought.	Products are certified by evaluation bodies to ensure that they have been built to standards.	

Product security ecosystem

- 1. Buyers must know what to demand
- 2. Developers must know how to build
- 3. There must be an ecosystem of evaluation.

