CASE STUDY **PrimeKey**

Leading open-source PKI software provider uses Cryptosense Analyzer to efficiently identify potential crypto and key-management vulnerabilities.

> We already use a variety of tools to ensure software quality, but we see security as an area of continuous improvement, and Cryptosense tools give us a cryptography-focused view that other tools can't provide. A strong statement in itself, given the fact that PrimeKey's teams of engineers work day in and day out with cryptography.
>
> **Tomas Gustavsson, CTO PrimeKey**

Headquartered in Stockholm, Sweden, PrimeKey Solutions develops and supports the most downloaded open source enterprise public-key infrastructure (PKI) software available, providing businesses and organisations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation.

Easy Integration

PKI is at the core of enterprise security, and relies on cryptography to securely manage keys, certificates and authorization. The core PrimeKey PKI offering, EJBCA, is an enterprise Java application consisting of hundreds of thousands of lines of code and linking with a number of libraries. Using Cryptosense Analyzer, the PrimeKey development team were able to test security of crypto use, key-management, randomness quality, and password storage across the application. "The Cryptosense tools leverage our existing test cases, so integration was straightforward", commented Gustavsson, "that means we can continue to use the tool to test new developments and catch problems early in the development cycle."

The Cryptosense tools work by tracing calls made by the application to cryptographic libraries during execution. The trace is recorded as an abstract logical model, which is then analyzed by Cryptosense software to detect both shallow crypto bugs like insecure algorithms and short keys as well as deeper cryptographic flaws that rely on interactions between operations over the course of an execution. The analysis algorithms are based on years of academic research by the Cryptosense founders as well as input from standards organisations, public results and in-house research.

Reassuring Users

Using the tool also helps raise awareness of crypto security issues among developers and helps to build a culture of best practice. "After investigating the issues found, we can also use the reports to explain to the clients and prospects how we manage cryptographic security", explains Gustavsson. "All our customers are security-sensitive, which makes this assurance important."

To find out more about PrimeKey's PKI solutions, visit www.primekey.se

EJBCA PKI by PrimeKey

Try it for yourself: **testmycrypto.com**

To find out how your organization can use Cryptosense to discover and mitigate unknown vulnerabilities in cryptography, contact us at **sales@cryptosense.com**

Cryptosense
MASTER CRYPTO RISK

Master Crypto Risk

1806 crypto misuse vulnerabilities added to the Mitre CVE database 2013 - 2015

83% of crypto bugs are in **applications**, not in cryptographic library code*

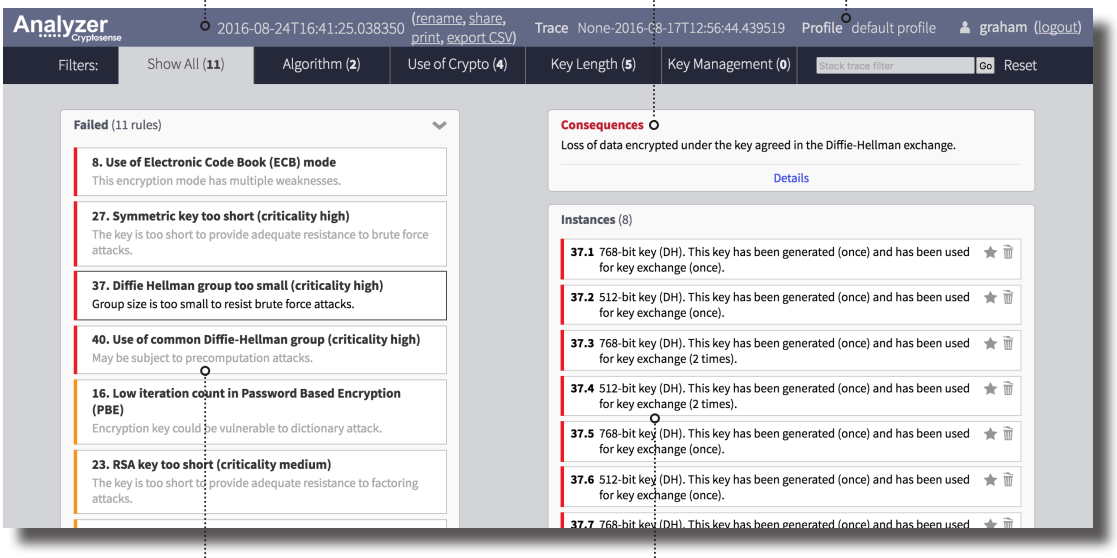
98.3% of crypto flaws **cannot be detected** by the best performing static analysis tool**

* *Lazar et al, Why does Cryptographic software fail? APSys '14*
** *2013 NIST SATE Evaluation*

Avoid failed evaluations with potential clients

Avoid being caught out by new crypto threats - latest results from academia

Export reports to demonstrate compliance



Covers all crypto including libraries & frameworks

Automation catches bugs early in dev cycle

* Use in-house or as SaaS

About Cryptosense

Cryptosense software allows our customers to find and fix security flaws in their cryptography. Thanks to our extensive, up-to-date crypto knowledge base and powerful analysis algorithms, our solution saves our customers time and money in securing the crypto used in their IT infrastructure and business applications.

Based in Paris, France, Cryptosense provides its solutions to the financial services industry, government agencies, and software and hardware producers.