The CrypTech Project

• Develop an open Hardware Security Module
  • Open hardware, software design
  • Support Applications such as:
    • DNSSEC
    • RPKI
    • TOR Consensus
    • Let’s Encrypt CA
• First complete machine – The CrypTech Alpha
The Cryptech CryRev Project

• Granted by NGI_Trust in the autumn 2019

• Develop a new revision of the Alpha improving:
  • Openness: Convert PCB design to KiCAD
  • Security 1: Move master key storage to FPGA with ns tamper response and key zeroisation
  • Security 2: Move all key related processing into the FPGA
  • Performance: Develop advanced RSA acceleration

A more open and trustworthy Cryptech HSM that provides competitive security and performance
CryRev Milestones

• January: Updated KiCAD board design
• March: Version 2.0 of the CrypTech board design
• April: Manufacturing test run of new boards
• June: New cores. SW etc. for V2 board validation
• August: Final SW for V2 board

Board design and finalization progress slowed due to COVID-19
CryRev Status (end of September) 1

• Finalization of Version 2.0 of the CrypTech board design
  • FPGA for Master Key Memory (MKM) and tamper integrated
  • Synchronous MCU-FPGA interface
  • Bug fixes

• Negotiation with board manufacturing in progress
  • ProPoint
CryRev Status (end of September) 2

- Official Release of CrypTech 4.0 – “way faster” in September
  - New high speed ModExpNG core with CRT and RSA blinding factor support
  - Clock FPGA synchronously from FMC bus with multipliers, to eliminate clock domain crossing bottlenecks
  - New AES-keywrap core with direct connection to master key memory
  - AES performance improvements
  - SHA-2 timing fixes to support higher clock rates
  - Redesign EC cores, adding support for ECDH (P-256 & P-384) and Ed25519
  - Support for hash-based post-quantum safe signatures

https://cryptech.is/2020/09/cryptech-releases-version-4-0/
CrypTech 4.0 RSA-2048 performance

- General version: 95 sigs/s
- Specialized signer version (no ECDSA): 130+ sigs/s
  - 7 parallel signer engines
- Single signer now 28+ sig/s
  - Really good for low cost applications

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>SafeNet USB HSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-1024</td>
<td>200</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>60</td>
</tr>
<tr>
<td>ECC P256</td>
<td>40</td>
</tr>
<tr>
<td>ECIES</td>
<td>20</td>
</tr>
<tr>
<td>AES-GCM</td>
<td>70</td>
</tr>
</tbody>
</table>
CrypTech Application Areas

• Automotive
  • HoliSec, CyRev identified need for in-vehicle key management
  • Secure onboard/offboard communication – ISO26262/ISO21434

• Maritime
  • NIS Directive

• IoT, ICS
  • Wireless Sensor Networks (Industriarmatur)
  • Distributed Control Loop
CrypTech Application Areas

• Identified Needs
  • Trusted Root, Trusted Storage, Key Management
  • Environment adapted solutions
    • New FPGAs for Automotive, ICS, Space from Xilinx
  • Performance, power, cost optimized
  • Reduced attack, problem surface

• CrypTech advantage
  • Highly flexible, modular design. Toolbox, platform
  • High performance single engine performance
  • Core for wrapping, at-rest protection of secrets (keys)
More information, Contact information

• CrypTech website: https://cryptech.is/

• Joachim Strömbergson
  • joachim.strombergson@assured.se
  • +46 73-375 97 02

• Jonas Magazinius – CEO Assured AB
  • jonas.magazinius@assured.se
  • +46 70-987 58 65
Tack!