What are the Alternatives to CySCoS?

At the time being, there is no other solution known to security demands, which is based on hardware architecture like CySCoS.
Therefore, CySCoS‘ competitors are

- **Trusted Platform Modules:**

This technology depends on an additional chip, holding cryptographical information, used to support authentication of software at system initialization. Compared with CySCoS, its disadvantages are:

  - Only one software or its provider is accepted.
  - Dependencies are durable and hard to change.
  - Authentication relies on a (considerably long) sequence of bits, which may be replicated by means of brute force.
  - No protection is provided against exploitation of
    - Stack overflows,
    - Spectre,
    - Meltdown
  - Control is deferred from the user due to the fact, that software configuration is restricted, as mentioned above.
  - Certain organizations, like the German Office for IT-security (BSI) regards this method as insecure (Ref.: Trusted Platform Module – Wikipedia [German Language]).

- **Secure Boot:**

This technology was invented to ensure, that computers are only booted with trustable firmware and operating system. This is done by the firmware checking digital signatures of boot loader and software components. If a signature is compromised or invalid, Secure Boot will not load that software. Compared with CySCoS, its disadvantages are:

  - No protection in case the certifying agency has been compromised.
  - The signature is subject to be bypassed by applying cryptographic means.
  - Secure Boot is activated or deactivated locally and manually by firmware-commands.
  - The state of Secure Boot (on/off) is not recognizable at system start.
  - It is Impossible to centrally activate/deactivate Secure Boot for several computers of an institution.
  - The German Office for IT-security (BSI): Secure Boot does not hinder or significantly complicate the exploitation of vulnerabilities. (Ref.: Sicherheitsanalyse der UEFI-Integration und Secure Boot-Implementierung von Windows 8 (bund.de) [German language]).

- **Antivirus- and similar software with well known disadvantages, as follows:**
  - They are only effective against known adversaries,
  - They do not recognize encrypted malware,
  - They are ineffective against future malware, and
  - They require frequent updates.
- **User directives, which have following weaknesses:**
  - Repeated instructions are necessary, especially after recognition of new threats,
  - Carelessness, especially during routine works,
  - Susceptibilities to
    - Curiosity,
    - Deception,

- Social Engineering, and
- Phishing