Protection of Components based on a Smart Card Enhanced Security Module

J. García-Alfaro[1,2], S. Castillo[1], J. Castellà-Roca,[3]
G. Navarro[1], and J. Borrell[1]

[1] Autonomous University of Barcelona,
Department of Information and Communications Engineering,
08193 Bellaterra - Spain

[2] Ecole Nationale Supérieure des Télécommunications de Bretagne,
Multimedia Networks and Services Department,
35576 Cesson Sévigné - France

[3] Rovira i Virgili University
Department of Computer Engineering and Maths,
43007 Tarragona - Spain

Introduction: Starting Point

- Protection of Network Security Components:
  - J. García, S. Castillo, G. Navarro, and J. Borrell
    Mechanisms for Attack Protection on a Prevention Framework
    39th Annual IEEE International Carnahan Conference on Security Technology
- Protection based on an AC integrated in the operating system's kernel
- Implemented as a Linux Security Module through the LSM framework

  $\Rightarrow$ Open architecture for the inclusion of security enhancements at operating system's kernel level

Introduction: Protection strategy

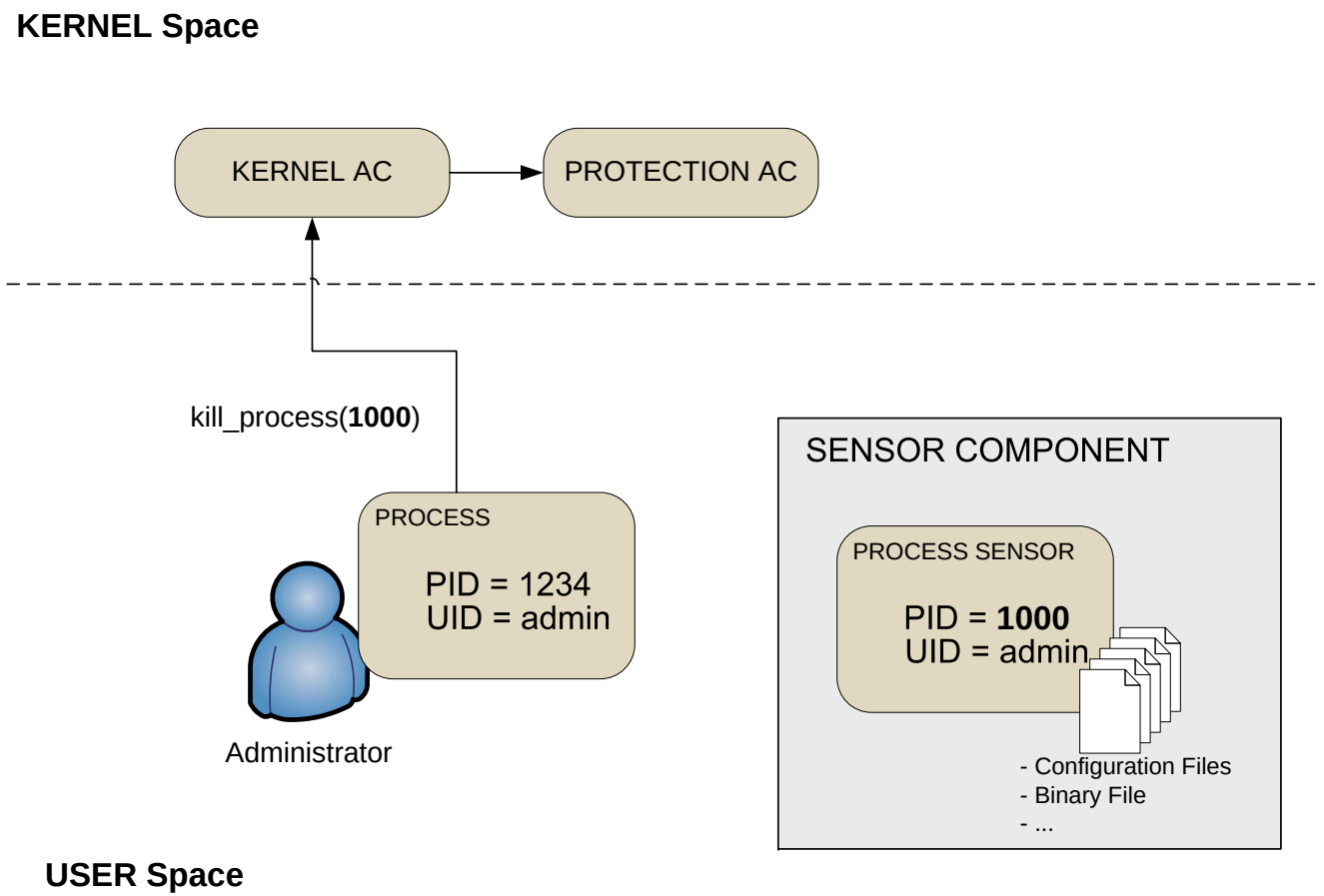
Introduction: Protection strategy

Intra-kernel Access Control

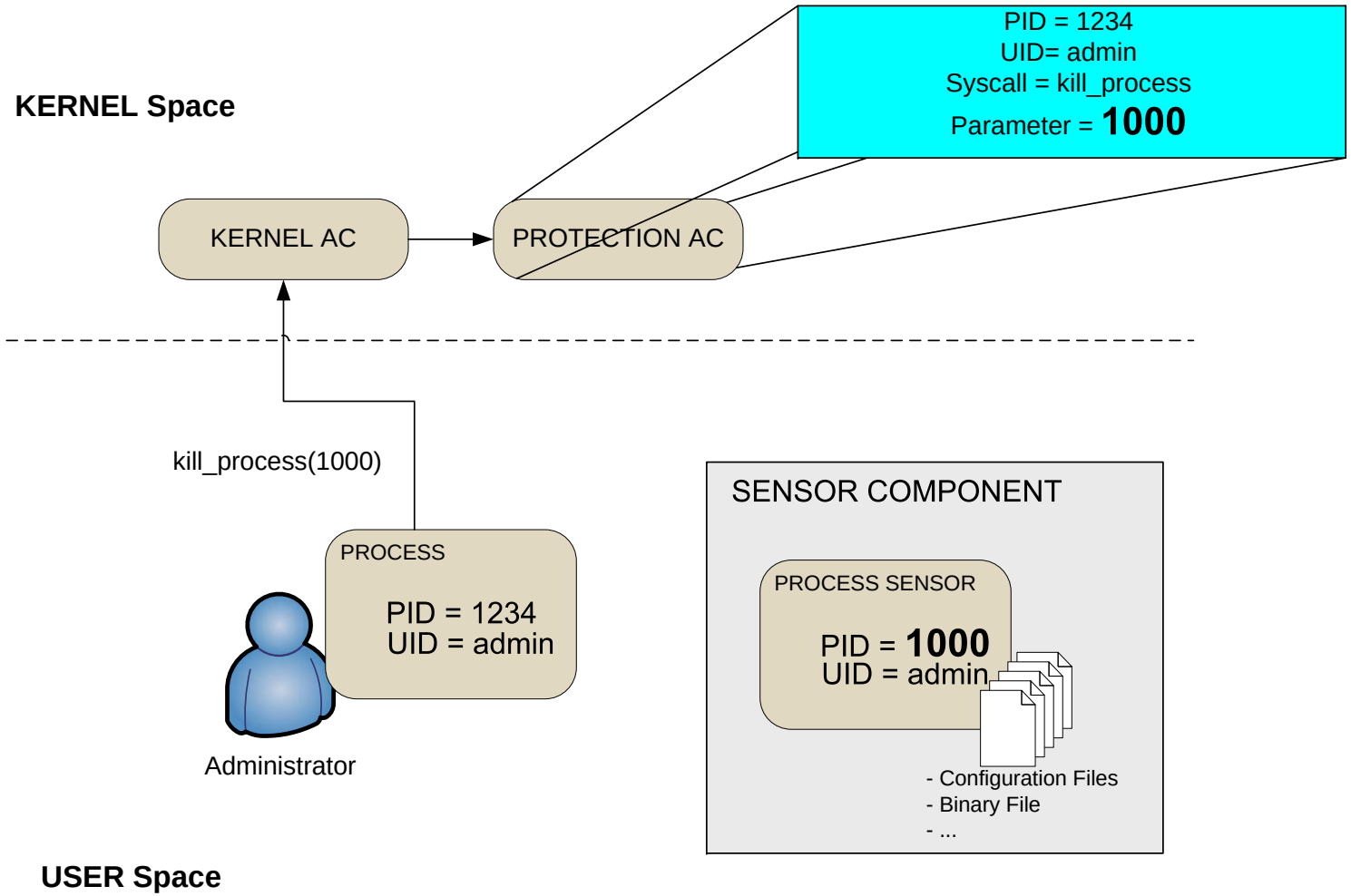
- Coexistence of the protection AC (more restrictive) with the native operating system AC (less restrictive)
- The protected system calls are intercepted and, according to a set of security rules, will be accepted or denied:

$$[\,PID\,]\,[\,UID]\,[Device]\,[inode]\,[Syscall]\,[Parameters]\;\rightarrow\;\{accept, deny\}$$

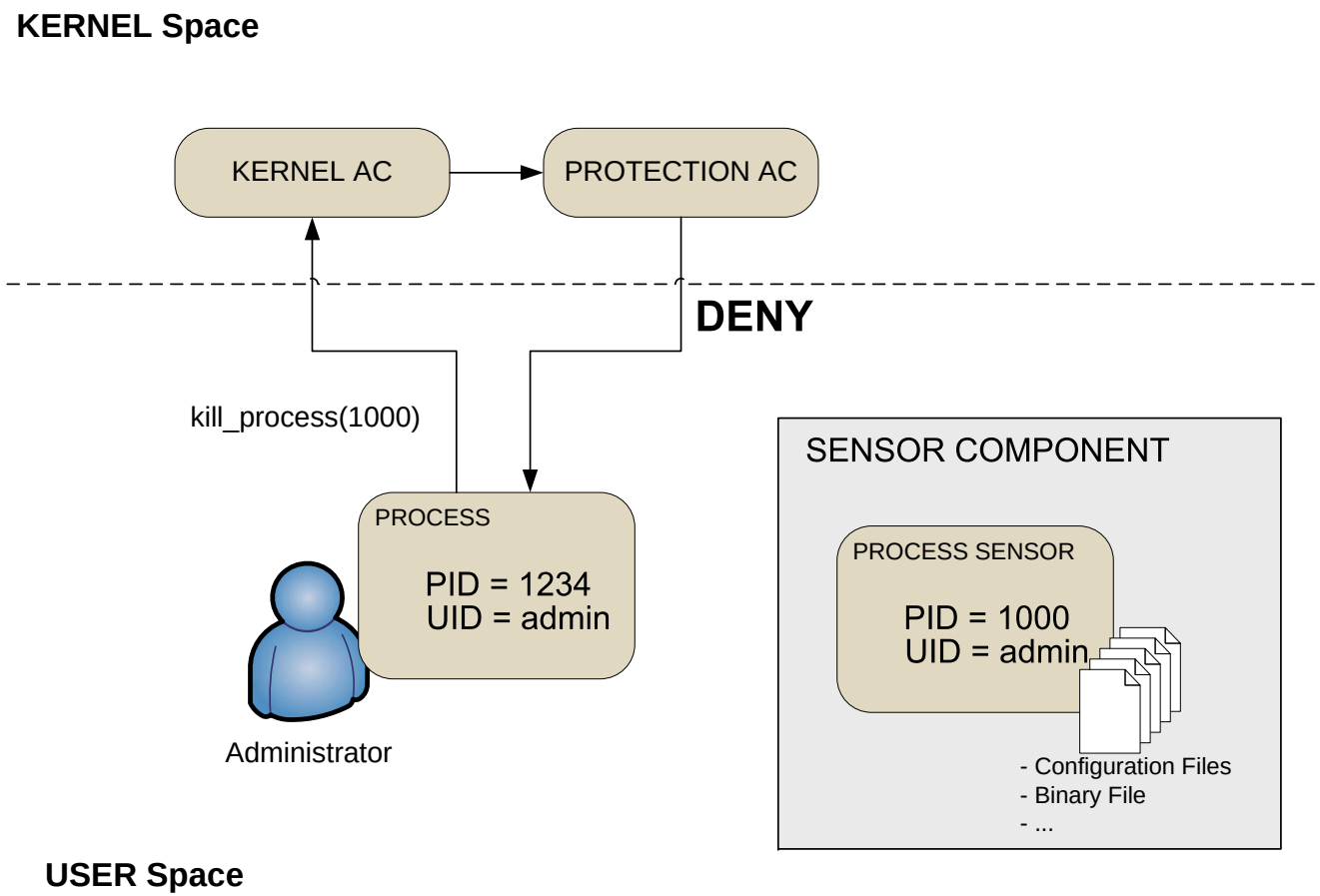
Example: protection of processes



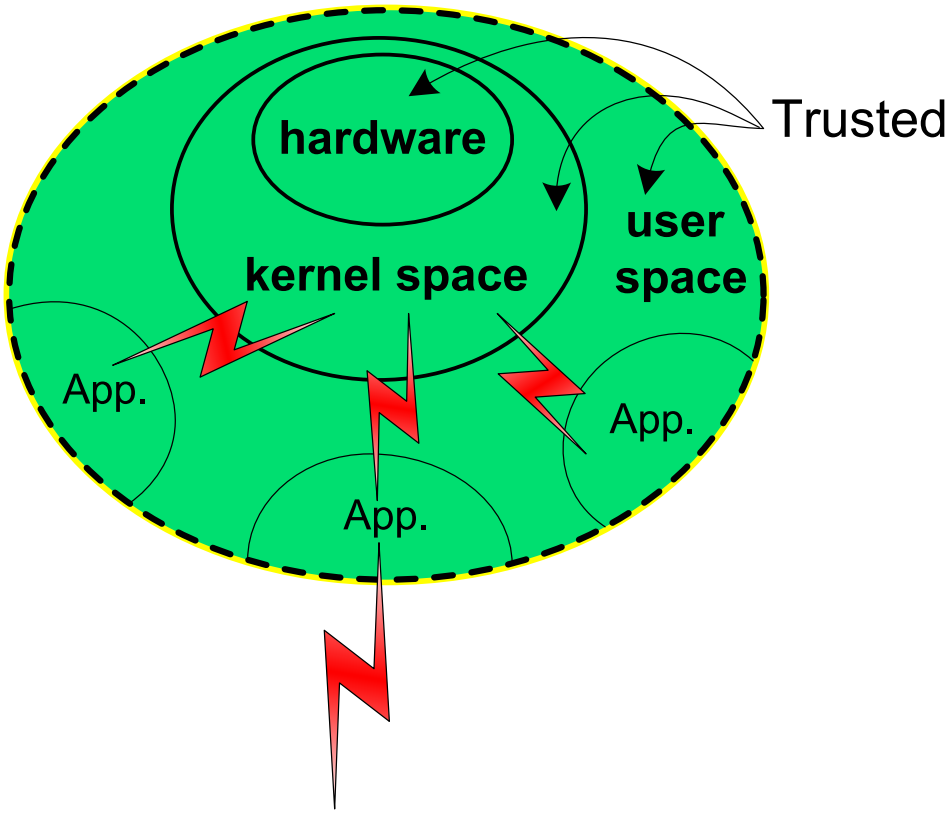
Example: protection of processes



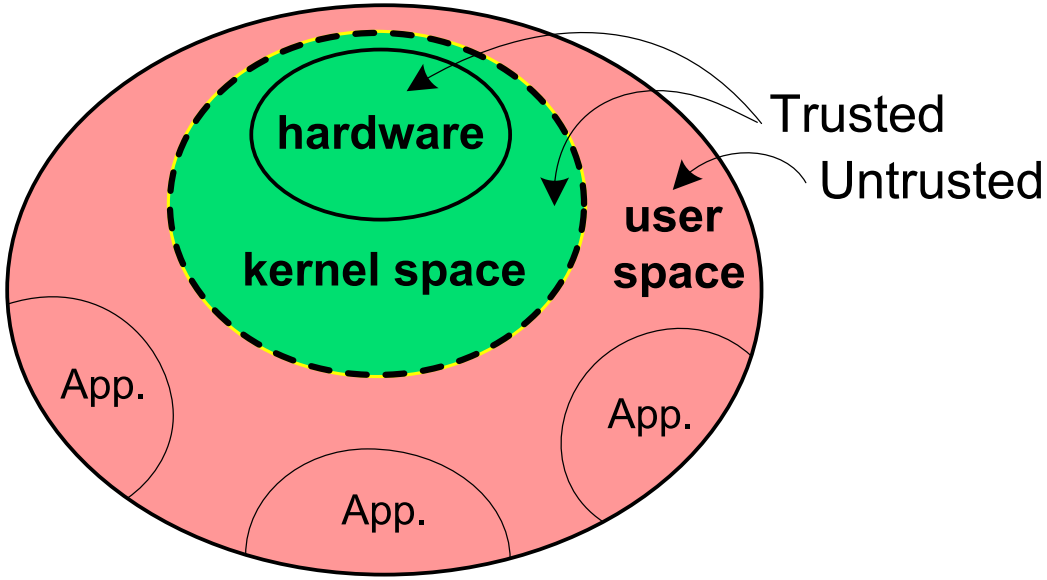
Example: protection of processes



Native operating system's AC



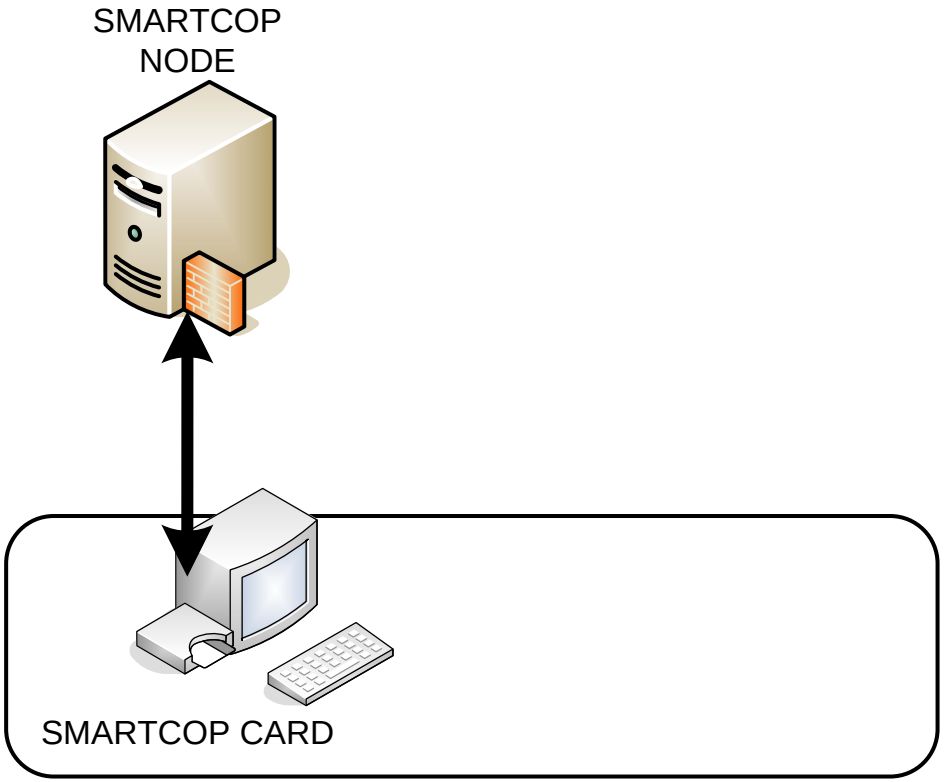
Intra-kernel Access Control



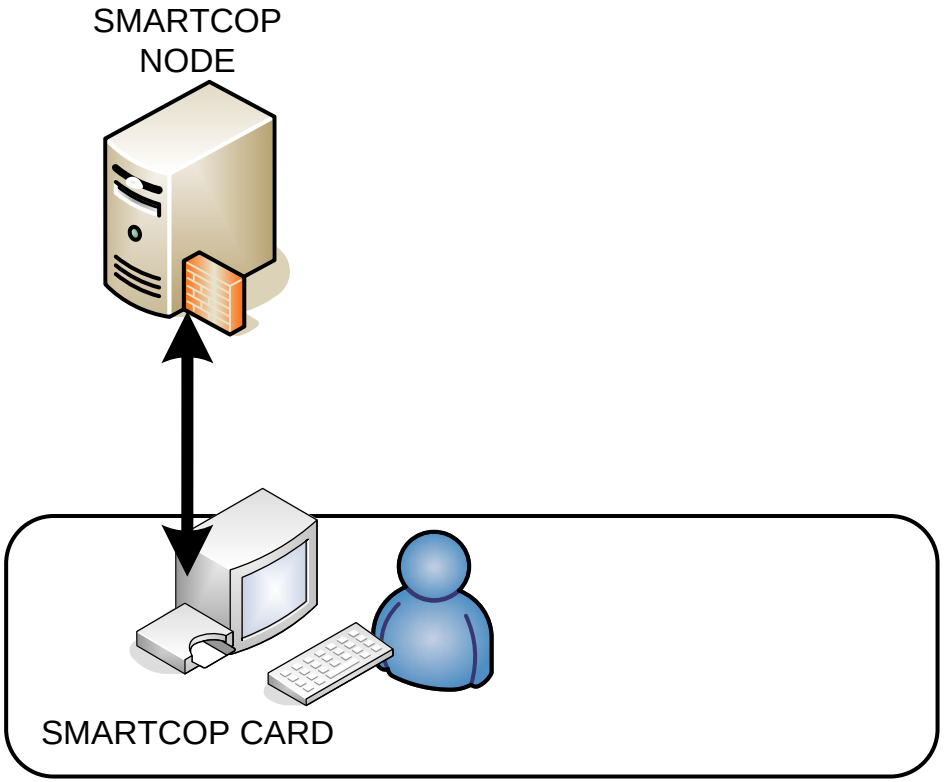
Constraints of our approach

- It introduces some administration constraints
  - $\Rightarrow$ Officers are not longer allowed to throw system calls which may suppose a threat to the protected component
- To solve these constraints, we propose the use of a two-factor authentication mechanism
  - $\Rightarrow$ Based on a cryptographic protocol and a smart card token
  - $\Rightarrow$ Holds to the officer the indispensable privileges to carry out management activities after ensuring the administrator's identity

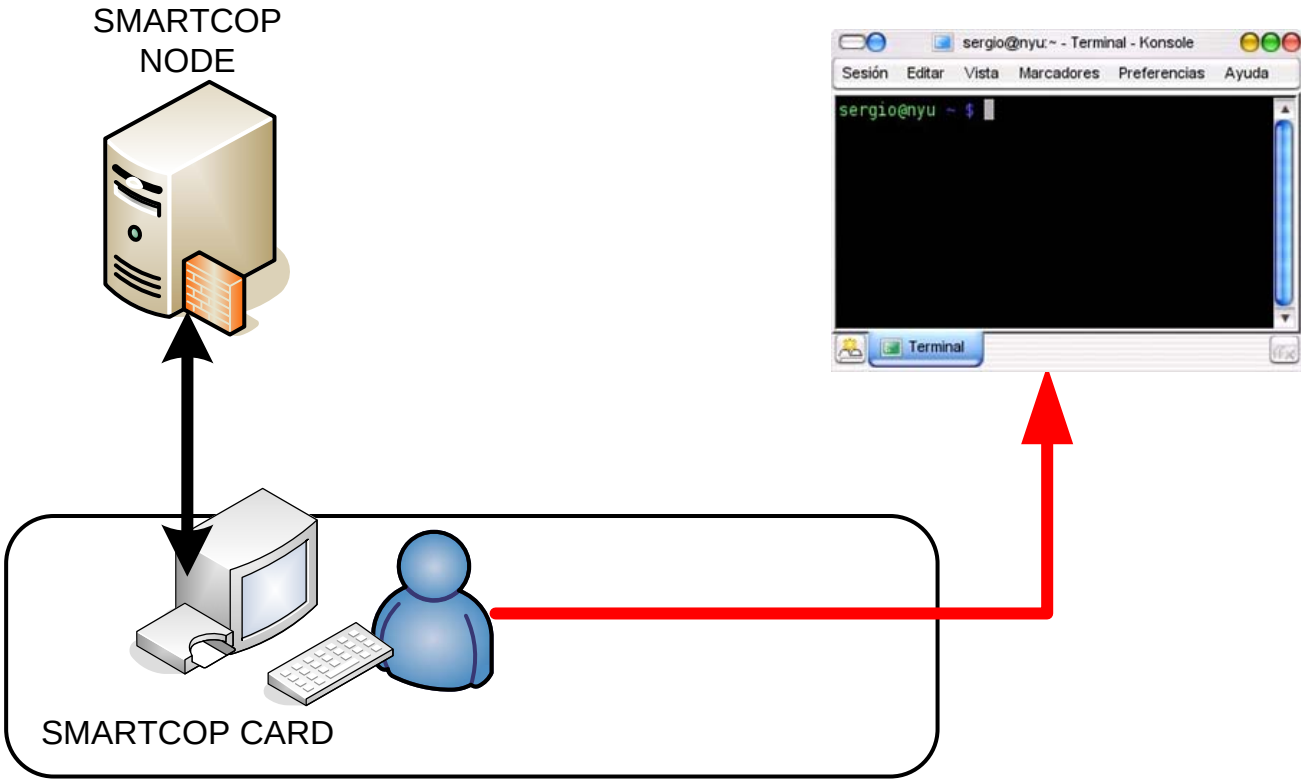
Authentication Mechanism



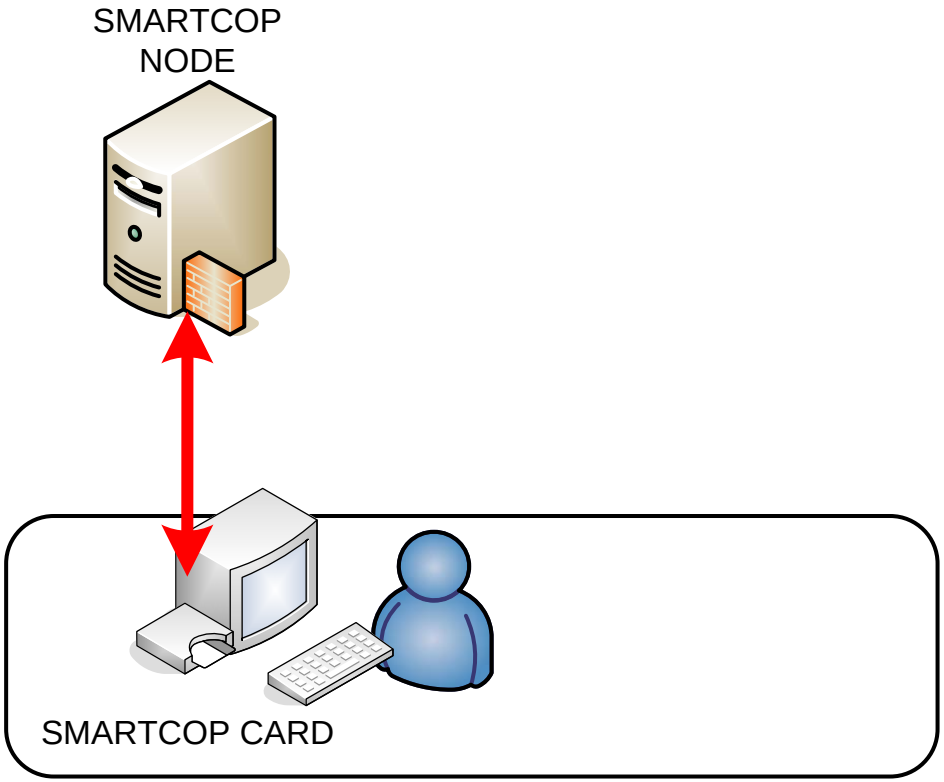
Authentication Mechanism



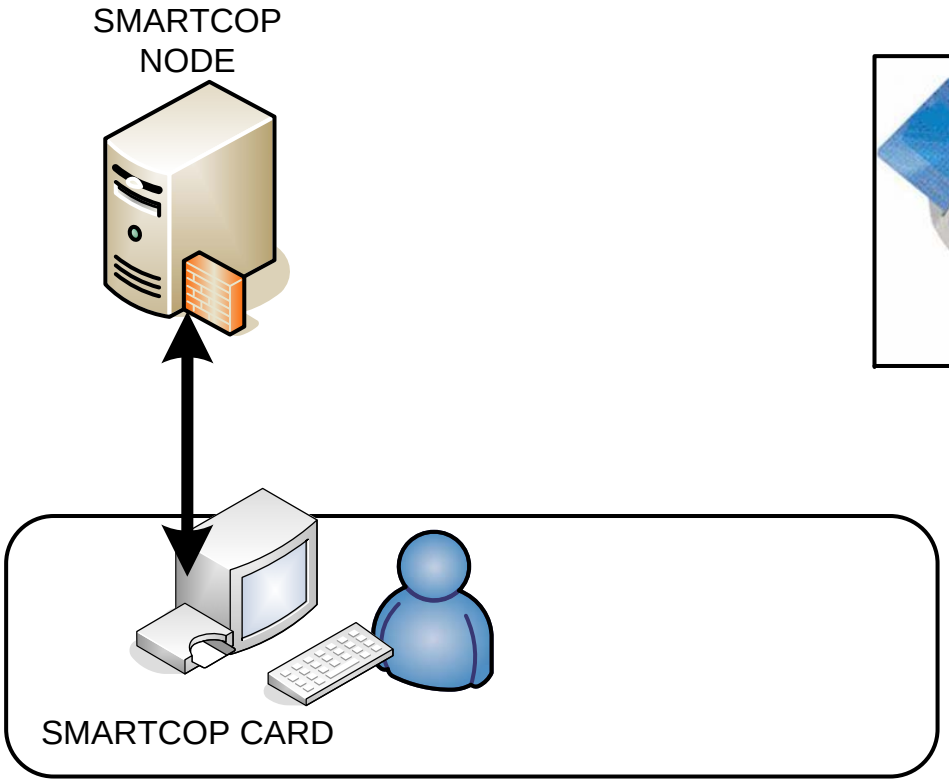
Authentication Mechanism



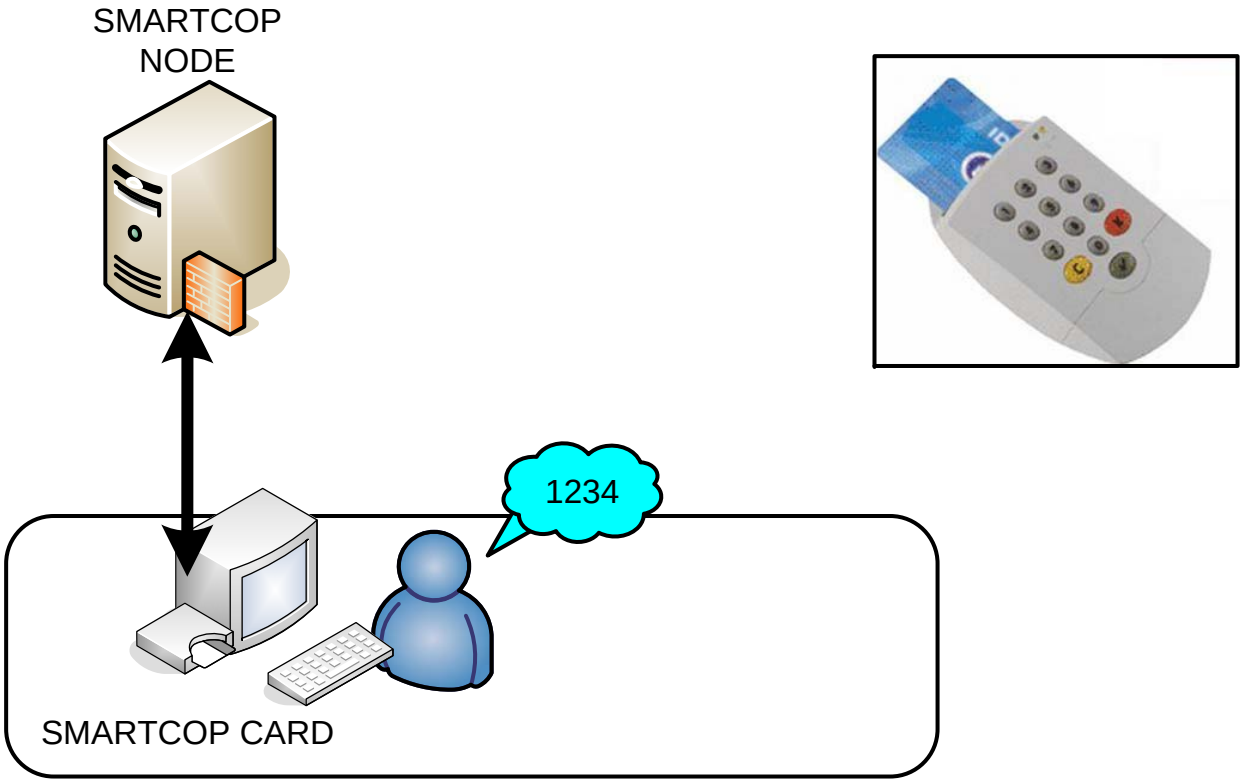
Authentication Mechanism



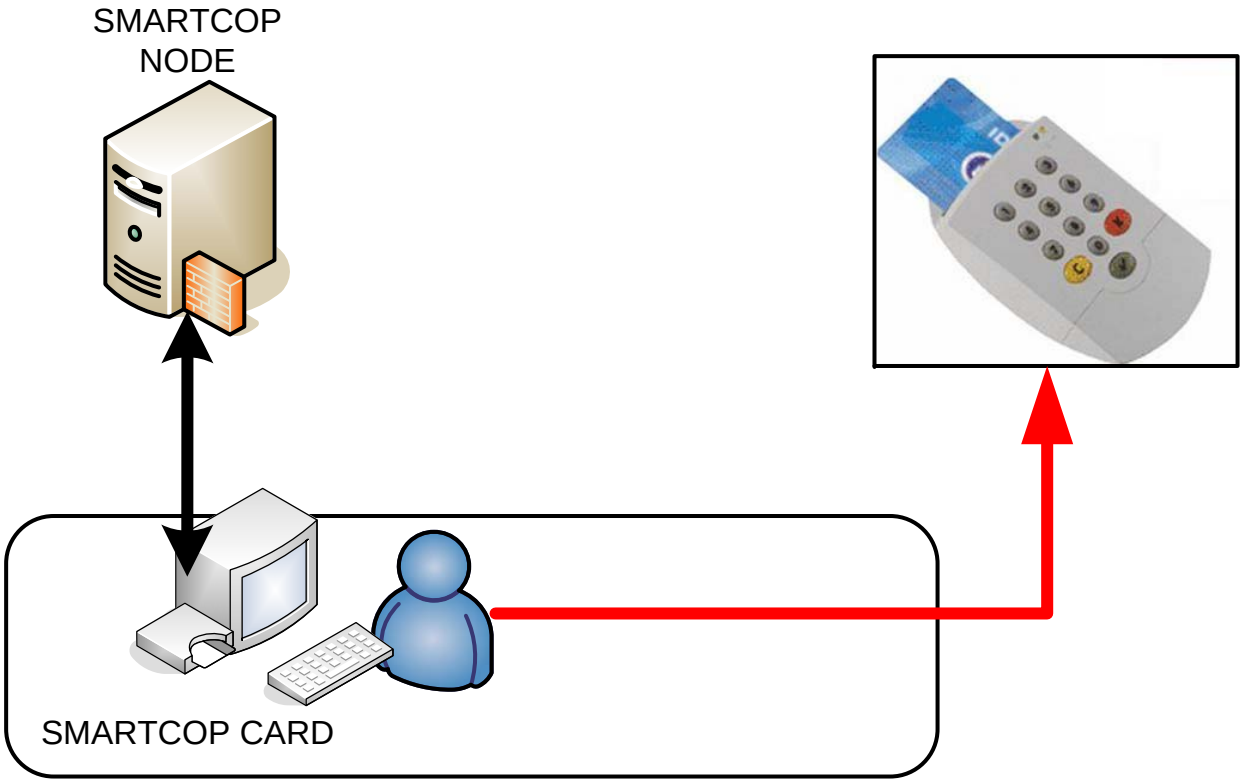
Authentication Mechanism



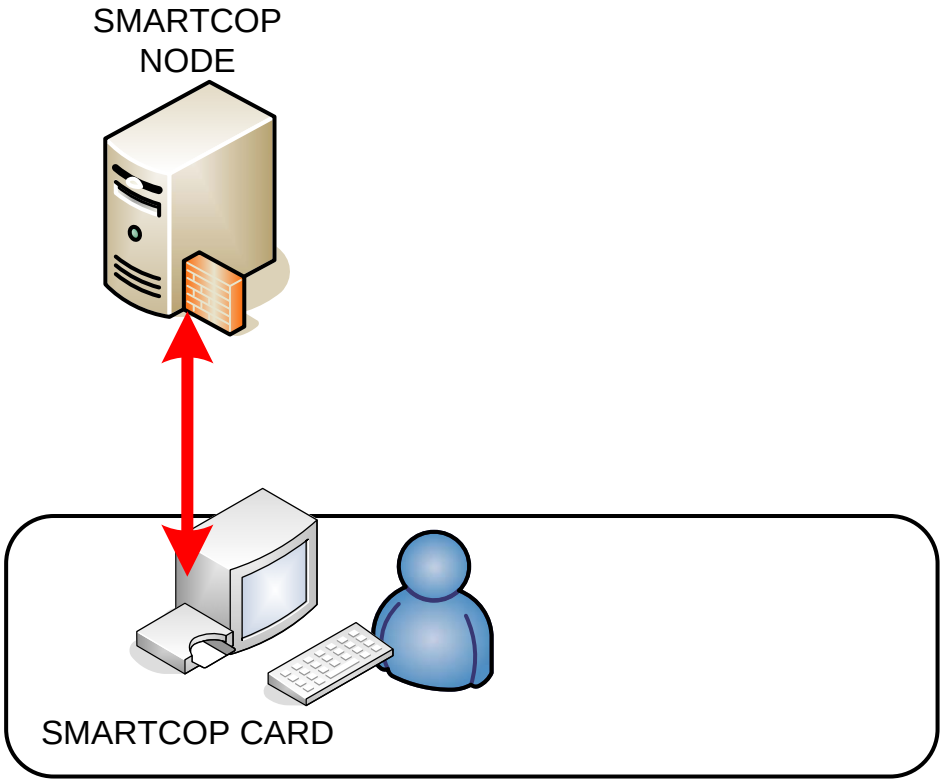
Authentication Mechanism



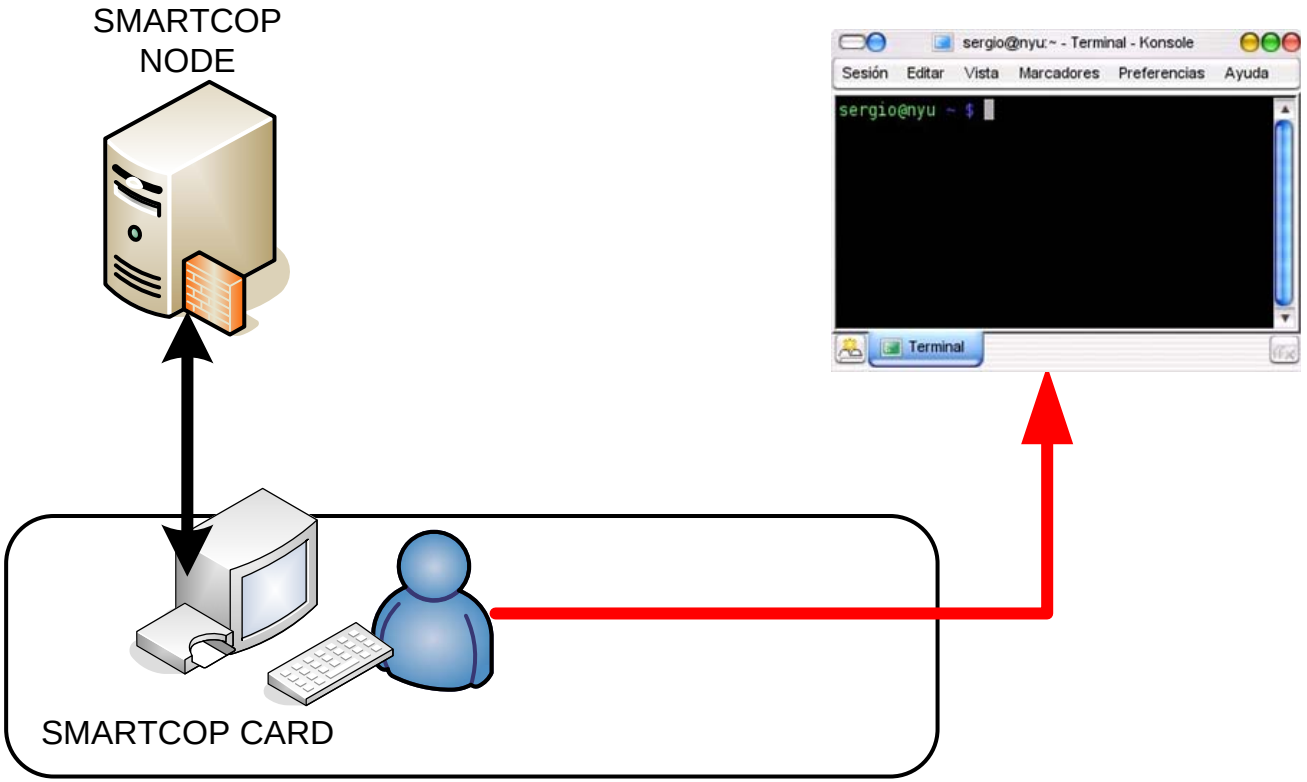
Authentication Mechanism



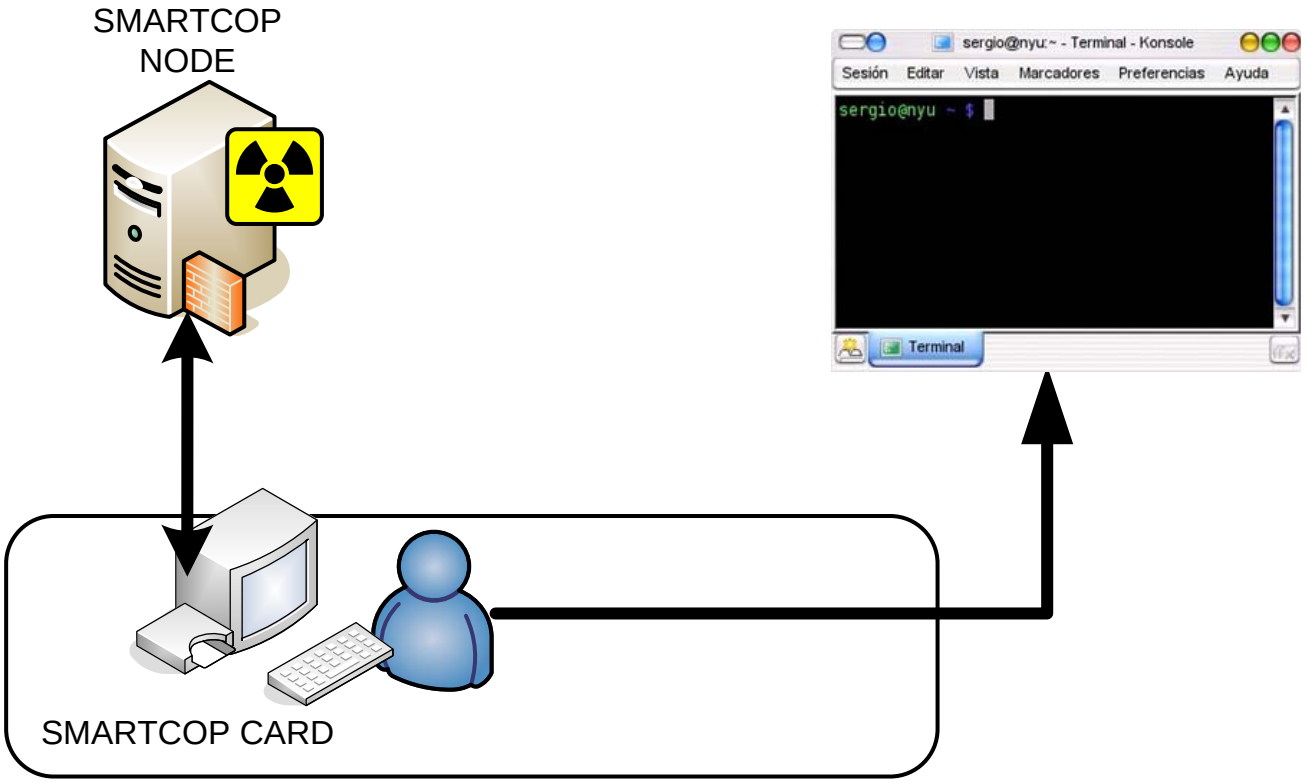
Authentication Mechanism



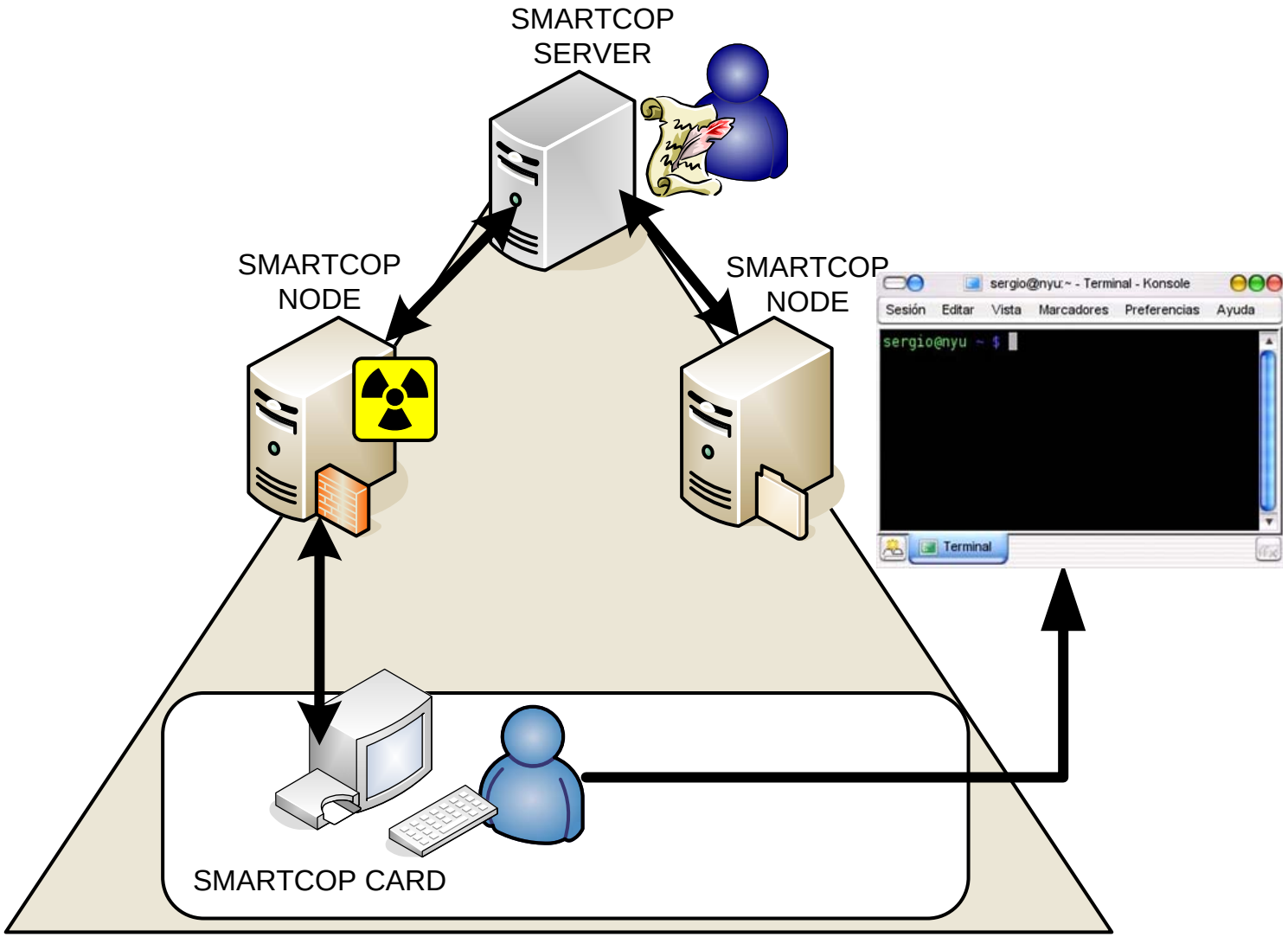
Authentication Mechanism



Authentication Mechanism



Public key protocol



Authentication Mechanism: security considerations

- The console's executable is compiled in a static manner
- The LSM module, moreover, protects:
  - the AC itself
  - the binary file of the console
  - the normal execution flow of the console's process
  - the communication channel between the LSM module, the smart-card, and the console process

Related Works

- SELINUX: P. Loscocco and S. Smalley. “Integrating Flexible Support for Security Policies into the Linux Operating System”. *11th FREENIX Track: 2001 USENIX Annual Technical Conference, USA, 2001*

- RSBAC: A. Ott. “The Role Compatibility Security Model”. *7th Nordic Workshop on Secure IT Systems (Nordsec 2002), Karlstad University, Sweden, 2002.*

  - Reinforce traditional operating system security features
  - Control of the outcoming system calls

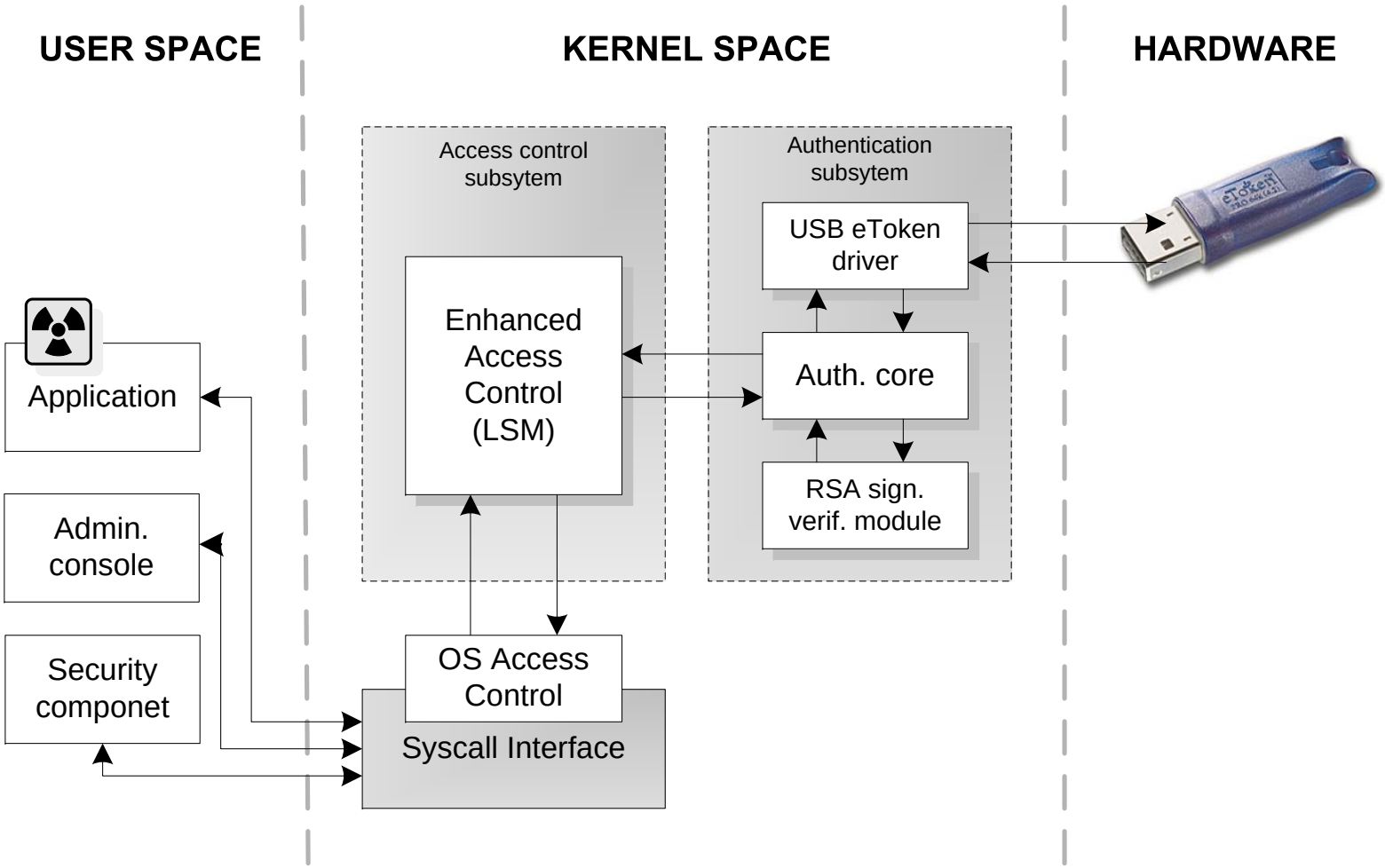
Benefits of our intra-kernel AC approach

- Unified methodology
  - $\Rightarrow$ Integrated in the system as a LSM module, without having to modifile and recompile the kernel
- Two-factor authentication mechanism
  - $\Rightarrow$ Solves the administration and configuration constraints of such an enhanced reinforcement

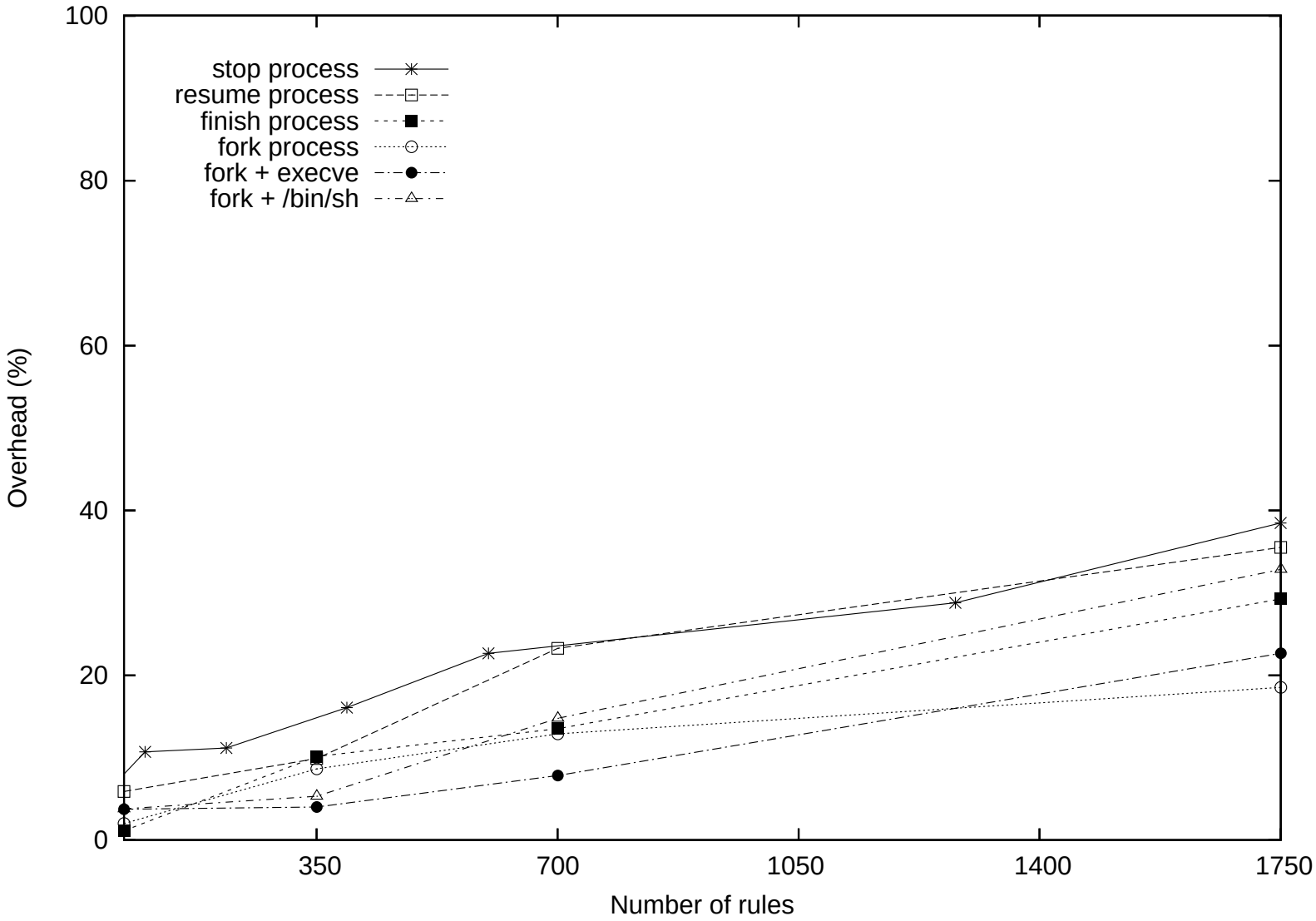
Deployment and Evaluation (1)

- Written in C as a set of modules through the LSM (*Linux Security Modules*) framework
- Smart card authentication:
  - $\Rightarrow$ LSM and smart card communication and cryptographic operations based on eToken PRO (Aladdin) cards
- Deployed over the components of our platform, implemented for *GNU/Linux 2.6* systems

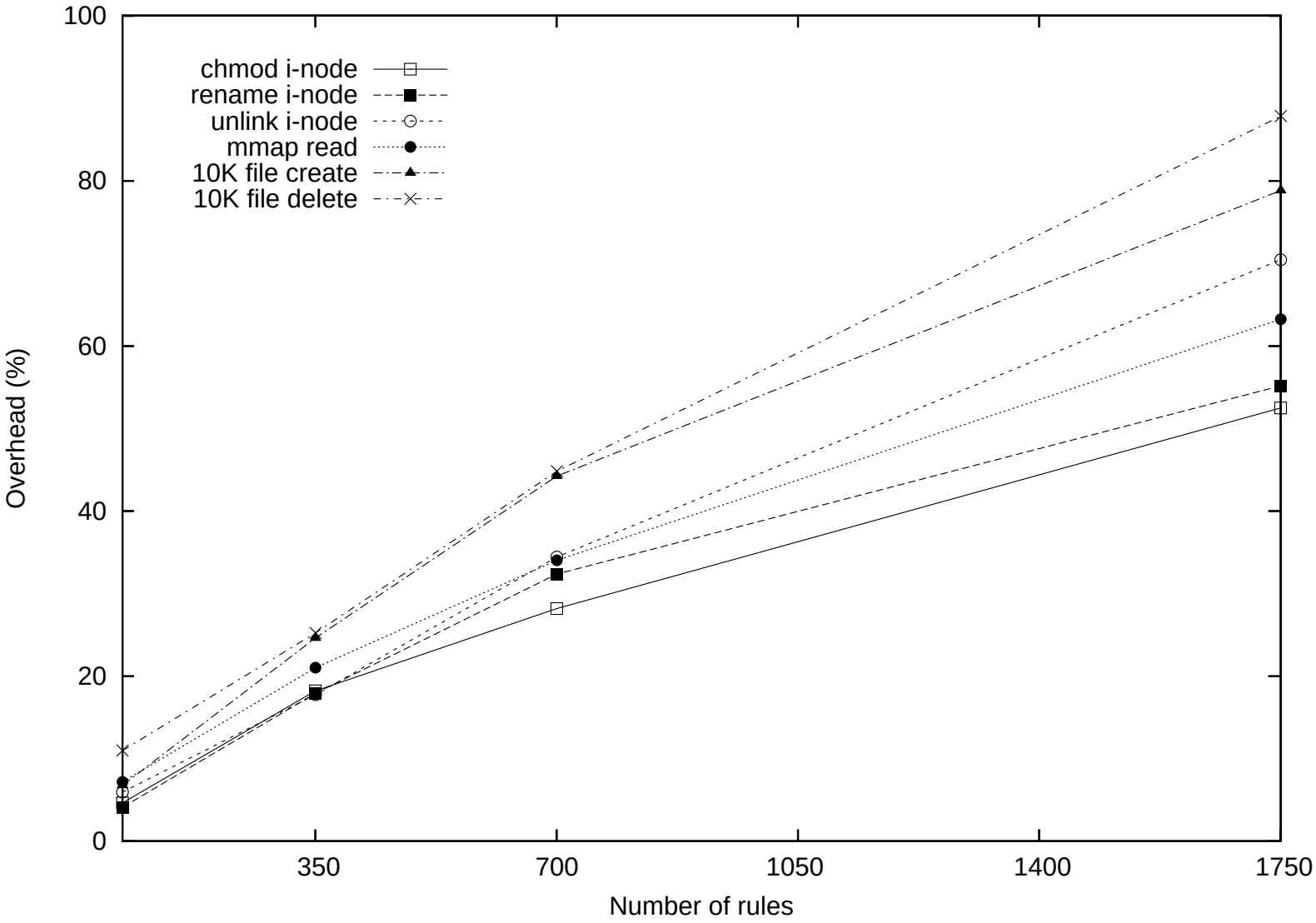
Deployment and Evaluation (2)



Evaluation: processes tests



Evaluation: filesystem and communications



Conclusions and Future Work

- **Conclusions:**
  - Protection of critical processes and resources based on an AC integrated into the operating system's kernel
  - Smart card based authentication protocol for management and configuration activities
  - Good degree of transparency and reasonable performance penalty
- **Future Work:**
  - Improving the customizing of policies
    $\Rightarrow$ Possibility of reload of policies at runtime
  - Improving the matching algorithm of security rules

Conclusions and Future Work

- **Conclusions:**
  - Protection of critical processes and resources based on an AC integrated into the operating system's kernel
  - Smart card based authentication protocol for management and configuration activities
  - Good degree of transparency and reasonable performance penalty
- **Future Work:**
  - Improving the customizing of policies
    - $\Rightarrow$ Possibility of reload of policies at runtime
  - Improving the matching algorithm of security rules

Thank you for your attention!

Questions?