

Secure Digital Criminal Dossier Management: combining local control and global access in distributed environments



IIDS Intelligent Interactive Distributed Systems

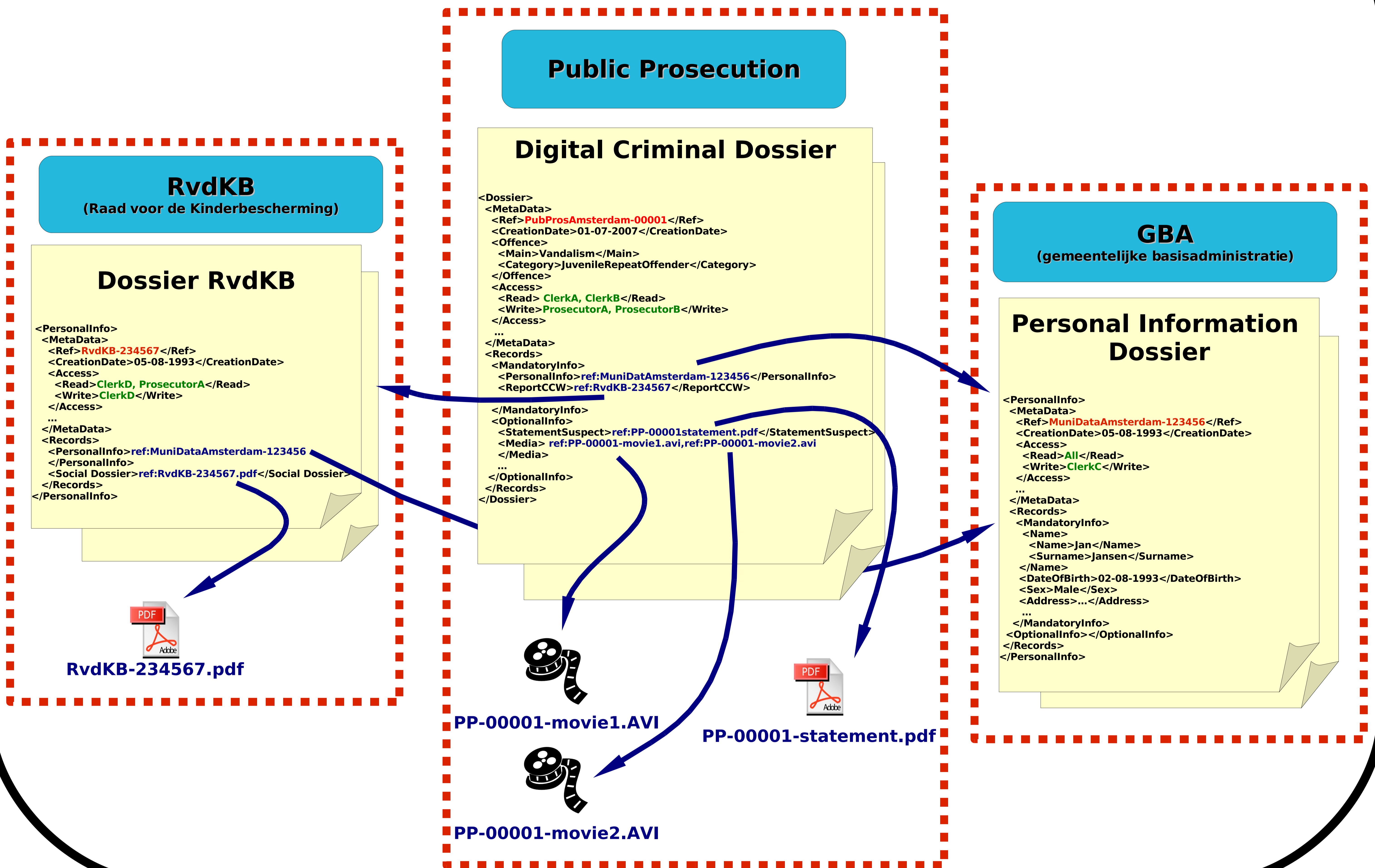
Martijn Warnier, Frances Brazier, Anja Oskamp

vrije Universiteit

amsterdam

www.iids.org/access

The notion of a *distributed digital criminal dossier* is central in the Agent-based Criminal Court Electronic Support Systems (ACCESS) project. Information is stored across organizations that remain responsible for their own information. Thus municipals (GBA) store administrative information on citizens, the prison systems store information related to (older) offenses and laboratories store information such as the blood-alcohol level of a suspect etc. The Public Prosecution creates a digital criminal dossier and refers to information stored at other organizations. This ensures that information stays as up to date as possible and that all organization maintain local control over (access to) their information, without hindering global information exchange.



Two tiered access control model

1. Role based access control (RBAC): all **Prosecutors** can read digital criminal dossiers
2. Access control lists (ACLs): **ProsecutorA** may alter information in digital criminal dossier **PubProsAmsterdam-00001**

The distinction between roles and individuals is crucial in a dynamic environment. Security policies based on roles can be regarded as *static* (or at least 'long lived') and are globally valid (at all possible locations), while individual access control lists are generally *dynamic* (or 'short lived'). Individual policies typically only apply per dossier, or even shorter, for example, when a criminal dossier is handed over to another clerk, prosecutor or judge.

- Local organizations use the static ACLs, which ensures **local control**.
- The system as a whole uses RBAC, which ensures **global access**

Other Key Features of the ACCESS project

- Criminal dossiers are distributed over numerous organizations, including the Public Prosecution, GBA, RvdKB, Probation officers, Prison systems and others.
- The infrastructure for managing digital criminal dossiers is based on multi agent systems. Agents perform modular tasks in this system including:
 - Enforcing the access control model
 - Checking completeness and consistency of dossiers
 - Assisting users (search etc.)
 - Guarding timeliness
 - Handling backups
 -
- Investigation and solving of legal constraints, such as:
 - Certain information in a criminal dossier is mandatory by Law (can be case dependent)
 - Some information may -by Law- be used only for a certain amount of time, for example until a juvenile suspect turns 18.



Computer/Law Institute
Vrije Universiteit



Netherlands Organisation for Scientific Research

