

Overview of the Persona Concept

Kal Toth, Assoc. Prof, Computer Science, Portland State University

Currently at the research and prototype stage, the “Persona Concept” is a web-based information sharing architecture supported by a personally held security device called the “Persona”. This concept is aimed at preventing on-line identity theft and protecting critical infrastructures including those for emergency response and law enforcement. The aim of the Persona Concept is to protect the confidentiality and integrity of both private and enterprise data while federating information access across end-user devices and across organizations. Rather than allowing access based on vulnerable password schemes, the Persona Concept makes use of electronic credentials to cryptographically access and authenticate information systems in accordance with personnel roles and attributes.

The Persona Concept is built around the user’s physical possession of a tamper-resistant device called the “Persona”. This device contains electronic credentials and software components that attest to the identity and attributes of its owner. The device itself may be a biometrically protected smart card, USB flash memory, SIM card or similar token that can be attached to a vehicle-mounted terminal, cell phone, PDA, or a desktop computer in the command center. The Persona thereby personalizes any terminal device to which it is attached and de-personalizes the device once it is removed.

The Persona is used to gain access to web-based systems provisioning vital services on behalf of collaborating organizations. Users from distinct organizations use their Persona devices to collaborate securely, sharing “sensitive but unclassified” (SBU) information in support of transactions and joint operations in both normal and emergency modes. In the context of emergency response and public safety, the Persona may be used to identify its owner, for example, a police officer, a fireman, an FBI agent, or a member of the coast guard. Credentials may also be allocated to identify individuals such as the local Police Chief, a firefighter in a particular district, the State Governor, the principal of a high school, or a senior administrator of a high-rise building.

The Persona Concept encompasses Persona devices, credential issuing services and web-based information systems using open web standards - “web-services” - as follows (see figure):

- **Establishing Security Policies:** Collaborating organizations establish both agency-wide and cross-agency security policies granting identity, role and attribute-based access permissions to services for their own personnel as well as personnel from collaborating agencies including public administrators (e.g. for receiving emergency alerts);
- **Electronic Credentials:** Identity, role and attribute credentials are expressed in the form of standard (XML-based) assertions that need to be placed in the hands of users to grant access. They can be revoked electronically at any time by issuing authorities to protect against various compromises including theft, misuse and role changes;
- **Issuing Credentials:** Each agency may issue its own credentials to their own personnel as well as to personnel from other collaborating agencies in accordance with both the agency’s and cross-agency (federated) security policies;
- **Distributing Credentials to Persona Devices:** Using web-based credential issuing services, collaborating agencies create and distribute electronic credentials to users by securely transferring credentials to their personally held Persona devices;
- **Accessing Agency Services:** Each user employs their Persona device to access authorized services provisioned by their own agency or affiliated agencies. Access is permitted when the electronic credentials stored in the Persona device are consistent with the security policies of the agency;
- **Authenticating Both Users and Agency Services:** The Persona device automatically uses the embedded electronic credentials to unambiguously authenticate the user to the agency’s web services as well as to authenticate the agency’s web services back to the user;
- **Encrypting Information Transfer:** To maintain confidentiality, the user’s electronic credentials are also used to encrypt all sensitive information and transactions transferred across the network.

Dr. Kal Toth, Associate Professor in Portland State University's Department of Computer Science, is the Associate Director of the Oregon Master of Software Engineering (OMSE) program and collaborates with the Oregon Regional Alliance for Infrastructure and Network Security (RAINS) www.oregonrains.org. He and his students have been conducting research and developing prototypes for the **Persona Concept** applying emerging software and web technologies and standards.

Web: www.cs.pdx.edu/~ktoth/ Email: ktoth@omse.pdx.edu

