**FAME – PERMIS**
Flexible Access Middleware Extension to PERMIS

**Introduction**
When users are accessing resources on the Web provided by different institutions, they are required to remember a username/password pair for each different resource provider. Likewise, resource providers are required to maintain lists of all users from various institutions requiring access to their resources. To resolve these access management issues, a strategy based on Shibboleth has been adopted among Virtual Organisations.

**Shibboleth**
- Defines a set of protocols for secure passing of identity information between users’ home institutions and service/resource providers.
- Relies on the home institution to establish the user’s identity and on the resource provider to grant access to the user based on the user’s attributes released by the home institution.
- The home institution authenticates its users using any authentication mechanism it supports.

- The target institution is only concerned with access control, thus users only reveal their true identity to their home institution that will release only minimal information about them that is necessary for the access control decision to be made by the target.

**FAME-PERMIS with Shibboleth**
- PERMIS is a policy-based access control engine that can be integrated with Shibboleth to help resource providers (targets) make their access control decisions.
- FAME is an extension to the Shibboleth on the home institution’s (identity provider’s) side, responsible for providing support for multi-factor authentication (e.g. by means of username-passwords, IP addresses, smart cards, soft certificate tokens, Kerberos, LDAP, etc.) and **Single Sign-On**.
- Each authentication method is assigned a Level of Assurance (LoA) according to its cryptographic strength. LoA is further passed via Shibboleth from an origin to a resource provider where it is fed into the PERMIS authorisation engine in order to include LoA into the target’s access control decision. This will enable security-sensitive resources to require users to authenticate with higher LoAs.

**Contact**
Dr. Ning Zhang, Uni. of Manchester (nzhang@cs.man.ac.uk)
Prof. David Chadwick, Uni. of Kent (d.w.chadwick@kent.ac.uk)