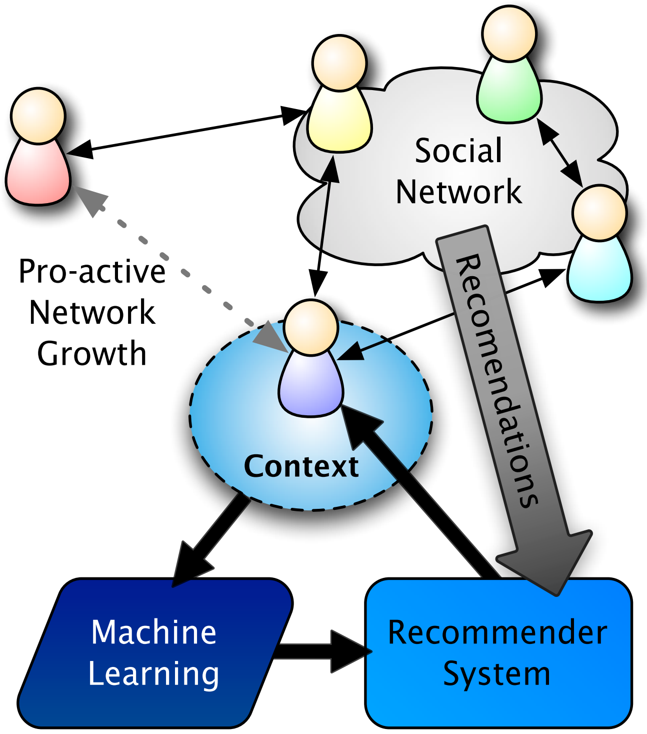
Virtual Centre of Excellence in
Mobile and Personal Communications

Mobile VCE

Instant Knowledge: Privacy & Security Brief

IK Concept

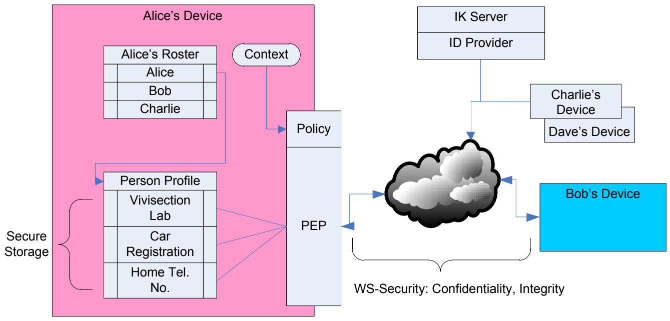
Instant Knowledge enhances the value of any organisation's most important asset—the information held by its employees. Rather than requiring staff to fill out skills profiles, which are very general, become outdated, and require significant effort, IK uses an application on employees' smart phones and laptops to gather information on what they are doing and who they are communicating with. This context is used to build dynamic skills profiles along with a social network map for the enterprise, which provides a resource to proactively offer recommendations to participants. Using IK, staff can always find the best person for the job.



IK Concept: It's not what you know, it's who you know, and who they know...

Privacy & Security Concept

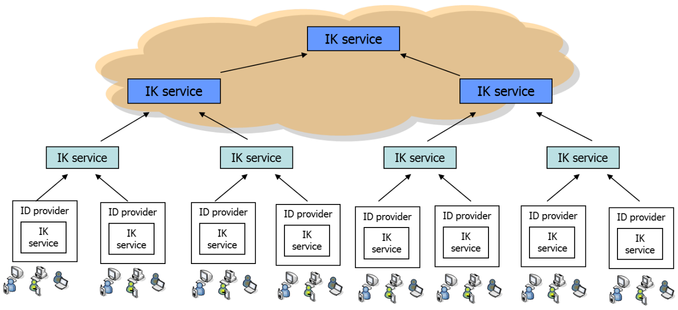
IK users' privacy is protected by providing 'privacy by design'. The privacy infrastructure exists by default. However the architecture is flexible enough to allow enterprises to choose which tools to apply and to allow users to determine local policy as required.



IK security architecture

Novelty & Contribution

Five privacy architectures were developed ranging from a simple centralised ID Management solution, where a trusted authority managed user pseudonyms, to a fully distributed solution. In addition to reversible pseudonymity, the latter provides k-anonymity by grouping users into clusters and forming a hierarchy of clusters.



Fully distributed privacy architecture

Industrial Chair: Glyn Jones, Thales UK Research and Technology **glyn.jones@thalesgroup.com**
Academic Coördinator: James Irvine, University of Strathclyde **j.m.irvine@strath.ac.uk**

Application Scenarios

Alice, Bob and Charlie are all legitimate users of the IK system. In this scenario, Alice is the victim of the attacks; Bob is Alice's boss; Charlie works in HR and is introduced to illustrate filtering of PII. In the IK system, Alice adds Bob and Charlie to her roster and consequently Bob and Charlie can see a subset of Alice's profile depending on Alice's privacy filter.

Daisy is a mutual friend of both Bob and Charlie and has at least two contacts in her roster: Bob and Charlie. However, Daisy does not know Alice. More importantly, Alice does not know anything about Daisy and the two have not formed a trust relationship. So although Alice is able to filter the release of PII based on trust relationships with Bob and Charlie, she cannot do the same for Daisy or any other IK user not in her roster.

Daisy may make genuine enquiries via IK and be given Alice's name by either Bob or Charlie in response. Thus, despite the privacy filter Daisy may be able to build a complete profile of Alice without Alice being aware of this.

The privacy architecture provides two mechanisms to mitigate this threat. Firstly, Bob and Charlie could give Daisy unlinkable pseudonyms for Alice (supported by signed credentials to validate any claims). Secondly, using k-anonymity, Alice could simply be introduced to Daisy as a member of Bob's team, without revealing her identity.

Demonstration Results

The security architecture was demonstrated using a Tomcat Application Server with J2SE, J2EE and JWSDP. The Mobile devices used J2ME and the MIDP 2.0 and SATSA extensions. Code was developed and using a J2ME Wireless Toolkit and Emulator from Sun.

The scenario demonstrated showed an IK knowledge provider with a secure profile of PII. Based on ID of IK requester, a subset of this PII was released and securely transferred to the requester. The IK Requester used the SATSA MIDlet to interact with network entities and Java Card.

A proof of concept privacy demonstration has been implemented on a Google Android platform to demonstrate two features of a potential privacy architecture: a decentralised identity management system operating with a centralised IK server and messaging system. Using a decentralised management system allows an enterprise to rapidly deploy an IK service by leveraging existing identity management infrastructure. To achieve this the Security Assertion Markup Language (SAML), developed by the Organisation for the Advancement of Structured Information Standards (OASIS), is used to build assertions that contain both authentication assertions as well as local policy authorisation decisions. These assertions are used by the IK service to determine the information that a particular IK user can request.

The centralised messaging system in the demonstration is managed using the concepts of reversible pseudonymity, as mentioned above. The demonstration system provides anonymity to both the IK user making a request and the IK user chosen to match that request; this can be adapted according to the requirements of the enterprise. A recommendation database is maintained that allows an authorised principal to determine an IK audit trail for purposes of information governance.

Conclusions

The IK project has developed a flexible privacy architecture built upon a secure end to end messaging system. The privacy architectures developed allow a separation of privacy policy from policy enforcement and may be deployed in a diversity of enterprise architectures. Moreover, privacy is built into the system by design and may be configured as required by each IK application.

Further Information

Videos and Technical Reports for all of the Instant Knowledge research outcomes are available to members on the Mobile VCE web site. For non-members the Instant Knowledge overview sheet is available at:

`www.mobilevce.com/infosheets/InstantKnowledge.pdf`

For further information and to register for information about future MVCE IK events please email Jerry Horton: **jerry.horton@mobilevce.com**